Workplace Monitoring in Asia, the Pacific and Japan

Report Prepared By:

Gary E. Clayton
Privacy Compliance Group, Inc.
8150 North Central Expressway
Suite 1900
Dallas, Texas 75206
214-365-1665
www.privacycg.com
gclayton@privacycg.com

PRIVACY COMPLIANCE GROUP, INC.

Workplace Monitoring in Asia, the Pacific and Japan

Notice

PCG is a privacy and data protection consulting company that works with leading companies and government agencies on the effective use of personally identifiable information. Although PCG may employ licensed attorneys and accountants, the information in this paper is not intended to be legal or accounting advice. If your organization requires such advice, you should consult your own professional adviser.

If you have questions or would like additional information on the matters discussed in this paper, please contact Gary E. Clayton at gclayton@privacycg.com or via telephone at (214) 365-1665.

Privacy Compliance Group, Inc.
February 7, 2008

Table of Contents

Workplace Monitoring in Asia, the Pacific and Japan

Introduction

The wide variety of privacy laws and regulations makes it difficult for companies to know what they can do to protect themselves, their employees, their networks and confidential information. For example, a company's ability to process, store, transfer and monitor their employees use of confidential information may vary greatly, depending upon where the data comes from and where it will be sent. Different countries apply different standards for the collection, processing and transfer of data.[1] As a result, it has become essential for United States ("US") companies operating internationally to understand the requirements for monitoring activities on their networks for each jurisdiction in which they operate. The purpose of this paper is to examine the requirements for workplace monitoring in Asia, the Pacific and Japan (collectively referred to as the Asia-Pacific Region ("**APAC**")). In particular, this paper will examine the requirements for workplace monitoring in the following jurisdictions:

- Australia
- Australia: New South Wales
- Australia: Victoria
- Australia: Capital Territory
- People's Republic of China
- Hong Kong (SAR)
- India
- Indonesia
- Japan
- Malaysia
- New Zealand
- Pakistan
- Philippines
- Singapore
- Republic of South Korea
- Taiwan
- Thailand
- Vietnam
- Singapore
- Republic of South Korea

This paper will also:

- Provide an overview of the international privacy standards that have formed the basis for many of the privacy laws in the APAC region.
- Examine the requirements for monitoring in the listed APAC economies.
- Examine the Privacy Framework that is being developed by the twenty-one member economies of the Asia-Pacific Economic Cooperation forum ("**APEC").**
- Examine how Vontu effectively safeguards employee privacy.

[1] '**Data**', as used in this paper, will refer to '**personally identifiable data**' that is defined as any information relating to an identified or identifiable individual. An individual is "identifiable' if they can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.

- Grade Vontu's safeguarding of employee privacy and the protection of confidential information.

This is the third in a series of papers examining issues related to workplace monitoring. The first paper, entitled **Protecting Confidential Information and Workplace Privacy**, provides a general overview focused on answering the question: "Can companies operating internationally monitor in the workplace?" The second paper, **Managing Workplace Monitoring in Europe**, provides an in-depth analysis focused on answering the question: "How do you monitor in the workplace in Europe?"[2] The current paper provides an in-depth analysis of the APAC region and is focused on answering the question: "How do you monitor in the workplace in APAC?"

Setting the Stage: An Overview of Privacy and Data Protection in APAC

Different Approach than EU

For over a decade, much of the debate in the privacy and data protection arena has focused on the significantly different approaches that the United States ('US') and European Union ('EU') have taken to protecting the privacy of their citizens. To date, the US has legislated privacy laws by industry sector. The US has eschewed comprehensive legislation and instead has relied on a combination of legislation, regulation and self-regulation. The EU, on the other hand, has adopted comprehensive principles that regulate all aspects of processing personal data. Indeed, EU's Data Protection Directive[3] ('Directive') is perhaps the best known and most influential privacy law in the world and its impact has been felt globally. The Directive requires the Member States to enact legislation to achieve the results of the Directive.[4]

By contrast, the economies[5] of APAC have taken a significantly different approach to the development of privacy and data protection protections. Rather than formal treaties, conventions or common constitutions, many of the countries of this region are developing regional laws based upon consensus and cooperation. Indeed, there are few, if any, legal requirements or constraints imposed. And, where there have been 'agreements,' they have been very different from the binding treaties or Directives of the EU.

Understanding how the privacy laws of the APAC region have developed is important to understanding the differences with the more legalistic and formalistic approach of the EU.

---

[2] For a copy of these white papers, please contact Vontu or visit www.vontu.com.

[3] Directive 95/46/EC of the European Parliament and of the Council on October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Although the Directive was enacted in 1995, it did not become effective until 1998.

[4] Ironically, the Directive itself is only a statement of EU policy – it is not the law itself. Instead, the EU Directive requires Member States to enact national legislation to protect personal data privacy and to appoint officials to enforce these privacy rights.

[5] The term 'economies' is used since members such as Hong Kong (SAR) are not countries.

This section will provide a brief overview of how the regional privacy efforts began and the two principle international frameworks that have shaped APAC privacy developments.

Efforts to develop a regional approach to privacy protections began in earnest in 2003 when Australia submitted a regional privacy proposal to the **Asia Pacific Economic Cooperation** ('**APEC**'). APEC is a voluntary international forum currently comprised of twenty-one members. APEC began in 1989, when Australia hosted the first annual meeting of Foreign and Trade Ministers from 12 Asia-Pacific economies to discuss ways to increase cooperation in this fast-expanding region of the world. Today, APEC has expanded to twenty-one members[6] that account for account for 57% of world GDP, 45% of world population and 50% of world trade.[7] If for no other reason than the sheer size of their joint economies, multinational companies must be aware of how these members regulate privacy.

History of APEC Privacy Framework

Ironically, Australia's efforts to develop an APAC regional approach to privacy grew out of its attempts to work with the EU on data privacy. Under the Directive, transfer of personal data to non-EU countries is allowed only if the receiving country provides 'adequate protection.'[8] In an effort to obtain such a finding, Australia's privacy laws were reviewed by the Article 29 Working Party, which is the independent EU Advisory Body on Data Protection and Privacy.[9] In January 2001 the Article 29 WP issued its opinion and found that Australia did not meet the EU's privacy standards and made a number of recommendations for changes to Australian law.[10]

At a meeting of the APEC E-Commerce Steering Group in Thailand in February 2003, Australia put forth a proposal for the development of APEC Privacy Principles using the OECD privacy principles as the starting point. The proposal reflected Australia's view that "there is no credible international standard other than the OECD Principles"[11] and dissatisfaction with the personal data export limitation approach by the EU Directive.[12]

The Organization of Economic and Cultural Development ('**OECD**') 1980 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data ('**OECD Guidelines**')[13] were the first international effort at addressing privacy, data protection and international transfers of personal data. The Guidelines set forth the following seven principles:

---

[6] APEC's current members are: Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong-China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States, and Vietnam.
[7] *See* APEC 2006, *available at* http://www.dfait-maeci.gc.ca/canada-apec/menu-en.asp.
[8] *See* Article 25 of the Directive.
[9] The tasks of the Article 29 Working Party are laid down in Article 30 of the Directive and in Article 14 of Directive 97/66/EC.
[10] *See* Article 29 Data Protection Working Party, Opinion 3/201 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000 (January 26, 2001), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp40en.pdf.
[11] Peter Ford, Implementing the Data Protection Directive - An Outside Perspective, (2003) 9 PLPR 141.
[12] For an in-depth discussion of the Australian approach, *see* Graham Greenleaf, *Australia's APEC Privacy Initiative: The Pros and Cons of 'OECD Lite*,' Cyberspace Law & Policy Center, University of New South Wales (May 15, 2003), *available at* http://www.bakercyberlawcentre.org/appcc/apec_ini.htm#fn4.
[13] *Available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

- **Collection Limitation**: "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[14]

- **Data Quality**: "Personal data should be relevant to the purpose for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date."[15]

- **Purpose Specification**: "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."[16]

- **Use Limitation**: "Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 [Purpose Specification Principle] of the OECD Privacy Guidelines except: (a) with the consent of the data subject; or (b) by the authority of law."[17]

- **Security Safeguards Principle**: "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data."[18]

- **Openness Principle**: "There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the Data Controller."[19]

- **Individual Participation Principle**: "An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; (iv) in a form that is readily intelligible to him; (c) to be given reasons if a request … is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended."[20]

- **Accountability Principle**: "A Data Controller should be accountable for complying with the measures which give effect to the principles stated above."[21]

---

[14] *Id.,* Paragraph 7.
[15] *Id.,* Paragraph 8.
[16] *Id.,* Paragraph 9.
[17] *Id.,* Paragraph 10.
[18] *Id.,* Paragraph 11.
[19] *Id.,* Paragraph 12.
[20] *Id.,* Paragraph 13.
[21] *Id.,* Paragraph 14.

According to the APEC Privacy Sub Group: "In many ways, the OECD Guidelines represent the international consensus on what constitutes honest and trustworthy treatment of personal information."[22] And, as discussed in the section below, the level of consensus on data privacy is particularly important in APEC which includes many nations that have limited or no history of privacy laws, such as Japan,[23] China,[24] Malaysia, Singapore,[25] Indonesia, Thailand and Vietnam.

Overview of APEC Privacy Framework

The APEC Privacy Framework is based around the OECD's Guidelines but are "expressed more simply and reflect three decades of experience in implementing those principles."[26] The APEC Privacy Framework also differs from the EU Directive in a number of key ways. First, under the APEC Framework, there is no formal mechanism to bind the APEC forum members to implementing the Framework into domestic legislation. Instead, consensus and cooperation are necessary for the effectiveness of the Framework. Second, the APEC Framework (like the OECD Guidelines) sets out general principles without the specific details found in the EU Directive. And third, business groups are playing a major role in the work of the APEC Electronic Commerce Steering Group, which oversees APEC's privacy-related initiatives. The involvement of private business groups is seen as balancing "information privacy with business needs and commercial interests, and at the same time, accord[ing] due recognition to cultural and other diversities that exist within member economies."[27]

The Privacy Framework contains nine information privacy principles:

- **Preventing Harm Principle**: [28] Interestingly, one of the key 'principles' of the APEC Privacy Framework is aimed at limiting the application of privacy protection rather than expanding upon a fundamental privacy right. The Preventing Harm Principle is intended to prevent the misuse of personal data. The principles focuses privacy protection on the practical impacts of the wrongful collection and processing of data. This is in sharp contrast to the more legalistic / fundamental human rights approach of the EU.

---

[22] APEC Privacy Sub-Group, *APEC Privacy Principles,* Version 9 (Consultation Draft), presented in Santiago, Chile, February 27, 2004, *available at* http://www.bakercyberlawcentre.org/appcc/apec_draft_v9.htm. A succinct presentation on APEC's privacy principles can be found at http://www.pcpd.org.hk/english/files/infocentre/1tonylam1_ppt.pdf.

[23] Since 2003, Japan has passed a series of privacy and data protection bills including the Act Concerning the Protection of Personal Information. Government agencies have also become involved in drawing up guidelines for protecting personal data.

[24] China's constitution contains limited protection of privacy but in fact, privacy in China has only been protected on a sporadic basis. The Special Administrative Region of Hong Kong has extensive privacy legislation and regulations.

[25] Singapore has no constitutional right to privacy and any common law rights are subordinated to the Government's efforts to preserve the social order.

[26] Tom Dixon, APEC Privacy Framework Progresses towards New Work on Cross-Border Information Flows, World Data Protection Report (November 2006).

[27] APEC Privacy Framework, par. 6 (2005) *available at* http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf.

[28] *Id.*at par. 14.

- **Notice Principle**:[29] The notice principle requires "clear and easily accessible statements" from the data controllers. The notices should address each of the following five issues: (1) the fact that the information is being collected; (2) the purposes for collection; (3) the types of organizations to whom the information may be disclosed; (4) the identity of the organization collecting the information and how to contact them; and (5) the choices that individuals have concerning the processing of the information. The Framework states notice should be given either before or at the time of collection – or as soon after as is practicable. Finally, the notice principle recognizes that it may not be appropriate for controllers to provide notice regarding the collection and use of publicly available information.

- **Collection Limitation Principle**: [30] The collection limitation principle states that personal information collected should be limited to information that is relevant to the purpose of collection and that any such information should be collected by lawful and fair means. Finally, "where appropriate", collection should be made with the consent of the individuals.

- **Uses of Personal Information Principle**:[31] The use of personal information principle provides that personal information should be used only to fulfill the purposes of collection and other compatible or related purposes. The only exceptions are: (a) the individual consents; (b) the processing is necessary to provide a service or product requested by the individual; or (c) by authority of law or legal instrument.

- **Choice Principle**:[32] This principle states: "where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information." The Framework notes that employees need not always be given choice regarding their employers' processing of their personal information. The Framework states:

  > "Further, in certain situations, ***it would not be practicable for employers to be subject to requirements to provide a mechanism to exercise choice related to the personal information of their employees when using such information for employment purposes***. For example, if an organization has decided to centralize human resources information, that organization should not be required to provide a mechanism to exercise choice to its employees before engaging in such activity."[33] (Emphasis added).

- **Integrity of Personal Information Principle**:[34] This principle requires personal information to be "accurate, complete and kept up-to-date to the extent necessary for the purposes of use." ***Note that the obligation to keep information accurate, complete and up-to-date is only required to the extent necessary for the purposes of use."*** [35]

---

[29] *Id.*at par. 15.
[30] *Id.*at par. 18.
[31] *Id.* at par. 19.
[32] *Id.* at par. 20.
[33] *Id*.
[34] *Id.* at par. 21.
[35] *Id*.

- **Security Safeguards Principle**:[36] This principle requires "appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses." The Framework also notes that such safeguards should be proportionate to the likelihood and sensitivity of the harm threatened, the sensitivity of the information and the context in which it is held. Finally, the safeguards should be subject to periodic review and reassessment.

- **Access and Correction Principle**:[37] This principle recognizes that an individual has three basic rights relating to their personal information: (1) the right to obtain confirmation of whether or not the personal information controller holds personal information about them; (2) the right to obtain that information in a reasonable timeframe at a charge that is not excessive; and (3) the right to challenge the accuracy of the information. The Framework Commentary notes: "The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right." The Framework notes that such access and opportunity should be provided except where "the burden or expense" of providing them "would be unreasonable or disproportionate to the risks to the individual's privacy." Additionally, there may be reasons not to provide access and correction where information relates legal issues, security considerations, the need to protect confidential commercial information or the privacy of another person. If a person's request for access or correction is refused, the controller should provide an explanation for that refusal *and* be able to challenge such denial.

- **Accountability Principle**:[38] This principle emphasizes two points: (1) it is the responsibility of the controller to comply with the privacy principles; and (2) when the information is to be transferred to another individual or entity, the controller should "obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will the information."

Regional Perspectives on Privacy

The APAC region touches on four continents and includes a wide variety of social, legal and cultural norms. As previously noted, the region includes a number of nations that have a very limited history of privacy laws such as Japan, China, Malaysia, Indonesia, Thailand and Vietnam. Others have had a relatively long experience in protecting privacy, including Hong Kong, Australia, New Zealand and South Korea. What this means for a multinational company is that employees in different offices throughout APAC may view the issue of privacy and monitoring in the workplace very differently based on their location.

[36] *Id.* at par. 22.
[37] *Id.* at par. 23.
[38] *Id.*at par. 26.

Based upon almost a decade of working with companies throughout APAC, it is recommended that multinational businesses take the time to understand the different social and cultural views on privacy and workplace monitoring. Additionally, companies should ensure that they understand the legal requirements for monitoring and determine the best way of providing notice and training to employees before implementing workplace monitoring. This will help avoid potential workplace issues and help your company provide the appropriate notice and training.

The following section analyses the privacy and data protection laws and regulations of a number of the APAC economies. The paper also examines the requirements for workplace monitoring in India and Pakistan. As you review the requirements listed below, it is important to remember that even where a country has no specific legal requirements that has to be met before workplace monitoring may take place, it is advisable to follow the general privacy principles listed in the APEC Framework. This is important not only for ensuring that your company complies with the developing regional framework requirements, but also because these principles largely represent what is considered "best practices' in the region.

^Back to Table of Contents^

>Listing of Country Laws>

Australia

General Privacy Laws	Personal Data Protection Laws	Workplace Privacy Laws
• Neither the Australian Federal Constitution nor the Constitutions of the six States and two Territories contain any express provisions relating to privacy. • The Australian Capital Territory adopted a bill of rights in 2004. Section 12 of the Human Rights Act of 2004[39] creates a right of "privacy and reputation."	• Principle federal statute on privacy is the Privacy Act of 1998, which is based in part upon the Organization for Economic Cooperation and Development ("OECD") Guidelines[40] and the International Covenant on Civil and Political Rights.[41] • Controls on the transfer of personal information out of the country are limited, requiring only that the data controller take "reasonable steps" to ensure personal information will be protected, or "reasonably believe" that the information will be subject to similar protection as applied in the Australian law. • The Office of the Federal Privacy Commissioner enforces the Privacy Act. This office has a wide range of functions, including handling complaints, auditing compliance, promoting awareness and advising the government on privacy matters. • There are numerous sector laws that regulate the use of personal information in special categories, such as health care, telecommunications, etc. • In March 2001, the European Union's Article 29 Working Party declined to find that Australia met the	• The Privacy Amendment Act of 2000[43] contains eleven Information Privacy Principles (NPPs) that require companies to observe the National Privacy Principles for Fair Handling of Personal Information.[44] • The Privacy Amendment (Private Sector) Act 2000 provides two important exemptions in its provisions that heavily impact the regulation of employment data protection. The first is the exemption for "small businesses"[45] and the second is the exemption of certain "acts and practices," including those related to employment records. Combined, these exemptions removed most employment data from the jurisdiction of the Privacy Act. It is important to note, however, that the Act contains exceptions for what qualifies as a "small business". Also, the Act authorizes small businesses to opt-in to be covered by the Act. As of 2007,

[39] Australian Capital Territory, Human Rights Act of 2004, *available at* http://www.legislation.act.gov.au/a/2004-5/current/pdf/2004-5.pdf.
[40] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.
[41] International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI) (Dec. 16, 1966), *available at* http://www.ohchr.org/english/law/ccpr.htm.

	requirements for providing "adequate protection" under the EU Data Protection Directive.[42]	almost 70 small businesses had opted to be covered by the Act. [46] • Employee records are defined broadly and include records that contain the types of personal information about employees typically held by employers on personnel and similar files. For example, a record containing information about the engagement, training, disciplining or resignation of an employee; the terms and conditions of employment of an employee; or an employee's performance or conduct would be considered to be an employee record for purposes of the legislation. • The exemption applies to acts or practices directly related to an employee record and a current or former employment relationship. This dual requirement is designed to ensure that employers do not take commercial advantage of the exemption.

[42] *See* Article 29 Working Party, Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000 (January 26, 2001) *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp40en.pdf.
[43] Australia Privacy Amendment (Private Sector) Act 2000, No. 155 (December 21, 2000), *available at* http://www.austlii.edu.au/au/legis/cth/num_act/pasa2000n1552000373/longtitle.html.
[44] *Id. extracted from* Australia Privacy Amendment (Privacy Sector) Act 2000, *available at* http://www.privacy.gov.au/publications/npps01.html.
[45] § 6D of the Federal Privacy Act provides: "A business is a small business at a time (test time) in a financial year (the current year) if its annual turnover for the previous financial year is $3,000,000 or less."
[46] Office of the Federal Privacy Commissioner, "Register of Businesses That Have Opted into Coverage by the National Privacy Principles," *available at* http://www.privacy.gov.au/publications/IS12_01.pdf.

Bottom Line: Generally, workplace monitoring is permitted by the "employee records exception" of the federal Privacy Act of 1998. The workplace monitoring should be proportionate to the risks addressed. Pursuant to the Federal Privacy Commissioner's Guidelines, the following are recommended for a company's privacy policy: (1) The policy should be promulgated to staff and management should ensure that it is known and understood by staff. Ideally the policy should be linked from a screen that the user sees when they log on to the network; (2) The policy should be explicit as to what activities are permitted and forbidden; (3) The policy should clearly set out what information is logged and who in the organization has rights to access the logs and content of staff e-mail and browsing activities; (4) The policy should refer to the organization's computer security policy. Improper use of e-mail may pose a threat to system security, the privacy of staff and others and the legal liability of the organization; (5) The policy should outline, in plain English, how the organization intends to monitor or audit staff compliance with its rules relating to acceptable usage of e-mail and web browsing; (6) The policy should be reviewed on a regular basis in order to keep up with the accelerating development of the Internet and information technology. The policy should be re-issued whenever significant change is made. This would help to reinforce the message to staff.

Discussion: On March 30, 2000, the Privacy Commissioner issued "Guidelines on Workplace E-mail, Web Browsing and Privacy," which discusses what should be included in the recommended privacy policy for a company. Companies wishing to conduct workplace monitoring in Australia should provide a clear notice to employees and, if practicable, obtain the employees written consent or acknowledgement. If employee personal data obtained during monitoring will be transferred to another country or to a third party, the notice should include this information. See the Privacy Commissioner's Guidelines for specific recommendations.

The Australians have traditionally looked to specific employment legislation to govern the rights of workers. On January 31, 2006, however, the Attorney-General of Australia asked the Australia Law Reform Commission (ALRC) to review Australian privacy laws and to make recommendations about ways in which they could be improved.[47] The ALRC is reviewing the federal Privacy Act. The ALRC's Final Report is scheduled to be completed March 31, 2008, and will contain the ALRC"s final recommendations for reform of Australia's privacy laws. The Final Report initially will be provided to the Attorney-General of Australia. It will then be publicly released within several months, when it is tabled in Parliament.[48]

[47] On January 30, 2006, the Attorney General issued the "Terms of Reference for Australian Law Reform Commission's scope of review. The Terms of Reference are available at http://www.alrc.gov.au/inquiries/current/privacy/terms.htm.

[48] *See* Australian Law Reform Commission's Review of ALRC issues Papers 31 & 32, Review of Privacy: Reviewing Australia's Privacy Laws – Is Privacy passé? . . . Have Your Say, (2007), *available at* http://www.austlii.edu.au/au/other/alrc/publications/issues/31-32_Overview/1.html#Heading1.

Australia: New South Wales

The Workplace Surveillance Act 2005 No. 47[49] became effective in the State of New South Wales, Australia on February 1, 2007. This legislation permits an employee to monitor employees' activities overtly, where the employees are given written notice of the manner, nature and duration of the surveillance. Covert surveillance may also take place where the employer has first obtained the necessary legal approval to do so. Surveillance will lawful and overt where an employer gives employees at least 14 days written notice of the surveillance before it begins. The notice **must** specify the following: (a) the type of surveillance that will be carried out (*e.g.,* computer, camera, etc.); (b) how the surveillance will be carried out; (c) when the surveillance will start; (d) whether the surveillance will be continuous or intermittent, and (e) whether the surveillance will be for a specified limit period or ongoing.[50]

Notice to New Employees: Section 10 of the Workplace Surveillance Act states that notice **must** be given at least 14 days before the surveillance commences, unless an employee agrees to a lesser period of notice. Section 10 also sets out the requirements for providing notice to new employees. Section 10 (3) provides: "If surveillance of employees at work for an employer has already commenced when an employee is first employed, the notice to that employee must be given before the employee starts work.

Computer Surveillance: Section 12 of the Workplace Surveillance Act states that computer surveillance must not be carried out unless: (a) the surveillance is carried out in accordance with a policy of the employer on computer surveillance of employees at work, and (b) the employee has been notified in advance of that policy in such a way that it is reasonable to assume that the employee is aware of and understands the policy.

Blocking Emails or Internet Access: Section 17 provides that an employer "must not prevent, or cause to be prevented, delivery of an email sent to or by, or access to an Internet website by, an employee of the employer, unless: (a) the employer is acting in accordance with a policy on email and Internet access that has been notified in advance to the employee in such a way that it is reasonable to assume that the employee is aware of and understands the policy; and (b) in addition, in the case of preventing of delivery of an email, the employee is given notice (a prevented delivery notice) as soon as practicable by the employer, by email or otherwise, that delivery of the email has been prevented, unless this section provides a prevented delivery notice is not required." The Act provides several practical exceptions to the requirements for the prevented delivery notice.

Use Limitations: The information captured as a result of surveillance can only be used or disclosed if: (a) the use of disclosure is for a legitimate purpose related to the employment of employees of the employer or the legitimate business activities or functions of the employer; (b) disclosure is to a member or officer of a law enforcement agency for use in connection with the detection, investigation or prosecution of a offense;

[49] *Available at* http://www.legislation.nsw.gov.au/fragview/inforce/act+47+2005+pt.5-TOP+0+N/?fragid=1&dq=.
[50] *Id.* at Section 10.

(c) the use of disclosure is for a purpose that is directly or indirectly related to the taking of civil or criminal proceedings; (d) the use or disclosure is reasonably believed to be necessary to avert imminent threat of serious violence to persons or of substantial damage to property.

Overt Video Surveillance: In New South Wales, overt video surveillance is regulated by the Code of Practice for the use of Overt Video Surveillance in the Workplace, issued by the New South Wales Department of Industrial Relations." Surveillance is "overt" if it is clearly visible to a person in the surveillance area.

Bottom Line: To conduct workplace monitoring in New South Wales, an employer must carefully follow the requirements of the Workplace Surveillance Act and: (1) adopt a policy regarding the use of company equipment, including emails and Internet, to ensure that employees are reasonably advised that monitoring will take place; (2) Describe the general details of monitoring and do so in writing; (3) Ensure that all employees are provided with at least 14 days notice prior to the commencement of monitoring; and (4) ensure that before new employees commence work, they are given written notice of surveillance at least 14 days prior to commencing employment. Employees should be informed as to the duration of the monitoring - and whether or not is will be for a specified limited period or ongoing. Once monitoring has started, the employer must ensure that the information captured is used only for the limited purposes set forth in the Act.

Australia: Capital Territory (ACT)

The federal Privacy Act in a slightly amended version applies to Australian Capital Territory government agencies and is administered by the Privacy Commissioner on behalf of the ACT government.

In 1992, the Australian Capital Territory enacted the Listening Devices Actwhich applies to "listening devices" and the interception of "conversations." There are a number of exceptions to this act, however, which allow parties with legitimate reasons to record private conversations.

In 2004, the Australian Capital Territory ("ACT") became the first Australian jurisdiction to incorporate a bill of rights when it passed the Human Rights Act of 2004 ("HRA").[51] Section 12 provides that everyone has the right "not to have his or her privacy, family, home or correspondence interfered with unlawfully or arbitrarily." HRA specifically incorporates international law and international human rights standards into local ACT law by requiring all ACT laws to be interpreted consistently with human rights "as far as possible."[52] It is likely that this new law will have an impact on all areas of privacy, including workplace monitoring. Pending further clarification, companies should follow the recommendations of the Australian Privacy Commissioner.

[51] *See* "An Act to Respect, Protect and Promote Human Rights (Human Rights Act 2004)", *available at* http://www.austlii.edu.au/au/legis/act/consol_act/hra2004148/ .
[52] *Id.* at Section 30.

Australia: Victoria

The Office of the Victorian Privacy Commissioner has provided guidance on workplace monitoring. Entitled "Workplace Privacy: April 2003", the Victorian Privacy Commissioner lists the laws and principles that employers must consider before engaging in monitoring. Among the laws that must be considered are the Surveillance Devices Act 1999 that controls the use of surveillance technology and restricts the communication and publication of private conversations and activities. In addition, Victoria's Information Privacy Act 2000 applies where personal information is recorded. This will include personal information in almost any format, including computer records, email and other electronic communications. In the Privacy Commissioner's Annual Report for 2006-2007, it is noted that a large number of complaints received by the Privacy Commissioner's Office related to monitoring in the workplace. The Privacy Commissioner's response is as follows: "For such enquiries, Privacy Victoria staff inform enquirers that even if the private sector employer does not fall within the small business exemption of the *Privacy Act* and is bound by it, the Act nevertheless contains an exemption in relation to personal information of employees. This is to ensure that the enquirer understands the limits of jurisdiction before being referred."[53]

On July 25, 2006, Victoria became the first Australian State to enact a Bill of Rights when the Victorian Parliament Passed the Victorian Charter of Human Rights and Responsibilities 2006. The Charter took legal effect on January 1, 2007. Section 13 of the Victorian Charter provides that a person has the right "not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with." It is likely that this Bill of Rights will have an impact on all areas of privacy, including workplace monitoring. In light of the exemption employee information from privacy legislation, it is not yet clear how the new Victorian law may impact the overall privacy rights of individuals if monitoring is lawful and not conducted arbitrarily.

People's Republic of China

General Privacy Laws	Personal Data Protection Laws	Workplace Privacy Laws

[53] Office of the Victoria Privacy Commissioner, *Annual Report: 2006-07* (October 2007), at p. 28 *available at* http://www.privacy.vic.gov.au/dir100/priweb.nsf/content/8B68E9EBB2F020DBCA256C6A007F820C?OpenDocument.

• There are limited rights to privacy in the Chinese Constitution.[54] • Article 38 of the Chinese Constitution states that the personal dignity of Chinese citizens is inviolable. • Articles 27 and 38 define the protection of freedom of the person and the residence. • Article 40 provides for the freedom and privacy of correspondence of the citizen.	• China does not have a general data protection law and there are very few laws that limit the government's ability to collect, use and disclose personal data. • China's Administration of E-mail Service Procedures protects the privacy of a citizen's email. The Procedures also provide that a person is only entitled to use a computer system to send e-mails if the owner of the system gives authorization. • China's General Principles of Criminal Law, Article 252 states that serious infringement of a citizen's right of communication freedom is punishable by prison time or placement in criminal detention.[55] • Article 7 of the Computer Information Network and Internet Security, Protection and Management Regulations states that the freedom and privacy of private network users may not be violated.[56] However, Articles 8, 10 and 13 requires individuals must be registered, that transferring accounts is prohibited, and all those engaged in Internet business are subject to security supervisions, inspection, and guidance, including assisting in incidents involving law violations and criminal activities involving information networks.[57] • Article 1(2) of the Administrative Measures on Safety and Protection of Computer Information Networks imposes affirmative obligations on companies to monitor computer and Internet activity on its equipment. • Articles 285 through 287 of the Criminal Code make unauthorized intrusions into computer systems	• China has no laws regulating or prohibiting workplace monitoring.[59]

[54] English translation of People's Republic of China Constitution is *available at* http://english.peopledaily.com.cn/constitution/constitution.html.

	illegal.[58]	
Bottom Line: The total absence of any law, regulations or jurisprudence on workplace monitoring provides no guidance to companies conducting business within the People's Republic of China. As a practical matter, companies that have internal global privacy policies should ensure that they follow their own policies and guidelines for workplace monitoring. While not specifically required, you should consider adopting a privacy policy stating that workplace monitoring will take place. The policy will ensure that employees have notice and will help ensure that monitoring is limited to what is authorized by the company. PCG recommends that the policy and/or guidelines state who approves monitoring and how and when it will be conducted.		
Discussion: Despite the absence of privacy laws in China, there have been efforts in the last few years to adopt data protection and privacy legislation.[60] In 2005, China's e-commerce legislation went into effect.[61] China has also been involved with the work on the Asia-Pacific Economic Cooperation Forum (APEC) on privacy rights.		

[55] English translation of Criminal Law of China, Part 1, Chapter IV, is *available at* http://www.cecc.gov/pages/newLaws/criminalLawENG.php.
[56] English translation of Computer Information Network and Internet Security, Protection and Management Regulations is *available at* http://web.archive.org/web/20041015045802/http://www.qis.net/chinalaw/prclaw54.htm.
[57] *Id.*
[58] General Principles of Criminal Law, Articles 285-287, *available at* http://web.archive.org/web/20041009190241/www.qis.net/chinalaw/prclaw60.htm. Article 285 limits only unauthorized intrusions into computer systems with "information concerning state affairs, construction of defense facilities, and sophisticated science and technology." *Id.*
[59] The Chinese Government routinely monitors Internet activity. For a description of censorship activities on the Internet, *see* Electronic Privacy Information Center, Privacy and Human Rights (2005), pp. 366 – 375.
[60] *See* Shi, Ting, "Landmark Privacy Law submitted for Review: Draft Legislation Sets out the Emerging Concept of Personal Data Protection," South China Morning Post, January 20, 2005.
[61] "*Ecommerce Legislation comes into Effect*," China Daily, April 1, 2005, *available at* http://www.china.org.cn/english/BAT/124412.htm.

Hong Kong (SAR)[62]

General Privacy Laws	Personal Data Protection Laws	Workplace Privacy Laws
• Article 29 of the Basic Law establishes the basic principle that homes of Hong Kong citizens are "inviolable."[63] • Article 30 of the Basic Law established the basic principle that the freedom and privacy of communication of Hong Kong residents is protected by law. No one shall infringe on the rights and freedom of privacy in communication except in accordance with legal requirements for protection of public security and the investigation of criminal offenses.[64]	• Personal Data (Privacy) Ordinance ("PDPO") came into effect in 1996, with the exception of the provisions concerning the transfer of data outside of Hong Kong[65] and data-matching.[66] • PDPO adopted six fair information practices to regulate notice, collection, accuracy, use, security and access regarding personal data which is defined as "any representation of information (including an expression of opinion) in any document, and includes a personal identifier."[67] The ordinance applies to public and private "data users" and to manual and electronic records. • Violations of the Ordinance can be either civil or criminal offenses. • The Office of the Privacy Commission has issued a number of codes of conduct, including the Privacy	• The Privacy Guidelines: Monitoring and Personal Data Privacy at Work provide guidance for assessing whether employee monitoring is appropriate and to determine how employers can develop privacy compliant practices in the management of personal data obtained form employee monitoring. • The Office of the Privacy Commissioner initially planned on releasing a statutory code of practice. However, strong opposition to the draft by employers made the PCO proceed with non-binding guidelines.[69] • The Guidelines verify that the PDPO applies to employee monitoring activities whereby personal data of

[62] On July 1, 1997, the People's Republic of China resumed possession of Hong Kong, establishing a "**Special Administrative Region**" ('**SAR**') and enacting a "Basic Law" (often referred to as a mini-constitution). The SAR was established in recognition of the "one country, two principles" concept, where the socialist form of government would not be practiced in Hong Kong. The laws of the Hong Kong SAR were incorporated into the Chinese legal system by the enactment of the Basic Law. An English version of the Basic Law is *available at* http://www.constitution.org/cons/hongkong.txt.
Under this arrangement, the Hong Kong SAR enjoys a high degree of autonomy in creating privacy-related legislation. Electronic Privacy Information Center, Privacy and Human Rights (2005), p. 523 (hereinafter referred to as "Privacy and Human Rights").
[63] Basic Law, *available at* http://www.constitution.org/cons/hongkong.txt.
[64] *Id.*
[65] Personal Data (Privacy) Ordinance, Chapter 486, § 33 (June 30, 1997) *available at* http://www.pco.org.hk/english/ordinance/ordglance.html.
[66] *Id.* at §§ 30-32. The provisions relating to data matching subsequently came into force on August 1, 1997.
[67] Personal Data (Privacy) Ordinance (Hong Kong), 1996, Chapter 486, § 2, "data."

	Guidelines: Monitoring and Personal Data Privacy at Work [68] (the "**Guidelines**").	employees is collected in recorded form. • Guidelines seek to offer practical guidance on the steps that should be taken by employers when they monitor employees using the following methods: telephone monitoring, Internet monitoring, video monitoring, and e-mail monitoring. • Guidelines recognize that an employer has the right to direct employees' work activities and to reasonably monitor such activities; however, monitoring should be balanced against the employees' right to privacy. • Guidelines provide that monitoring should take into account the following: 1. **Legitimate Purpose**: Monitoring should serve a legitimate purpose that relates to a given function and should be confined to include only the activities of the employees at work. 2. **Least Intrusive Method**: Monitoring should be carried out by the least intrusive means and with the least harm to the privacy

[68] *Available at* http://www.pcpd.org.hk/english/ordinance/files/monguide_e.pdf.
[69] R. Rodwell, "Guidelines push privacy issues to the forefront; Incorrect monitoring in the workplace can quickly sour employer-staff relationships." South China Morning Post, January 8, 2005, *cited in* Privacy and Human Rights, p. 533.

		interests of employees. 3. **Transparency**: Employers are encouraged to document the evaluation process they have undertaken and share it with their employees, in order to indicate transparency and inform employees of the rationale behind the monitoring. 4. **Targeted**: Monitoring should be confined as much as possible to include only high risk areas of the business and conducted selectively at certain times (rather than on a perpetual basis). 5. **Stated Purpose**: Monitoring should be conducted in an overt manner and for reasons identified in advance of monitoring. 6. **Limitations**: Monitoring should not take place in areas that contain a reasonable expectation of privacy (i.e., washroom). • Employers who monitor are accountable for properly conducting their monitoring activities, including the creation of a privacy policy pertaining to employee monitoring. The policy should be given to employees before monitoring is introduced.

		• Employers are liable for the provisions of the PDPO for the proper management of personal data collected while conducting employee monitoring. The legal obligation extends to acts and practices undertaken by a third party acting on behalf of the employer.
		
		• Employers should be aware that their employee monitoring practices may be subject to investigation by the Commissioner in any alleged breach of the PDPO. Investigation would ask employer to provide evidence of the following:
		
		  • Monitoring is only carried out to the extent necessary to deal with the legitimate business purpose of the employer.
		
		  • Personal data collected in the course of monitoring is kept to an absolute minimum and is collected by means that are fair in the circumstances.
		
		  • A written policy showing that employee monitoring has been implemented and that steps have been taken to communicate that policy to employees in advance of monitoring.
		
		  • Additional best practices, including designation of personnel authorized

		to conduct monitoring, criteria for accessing monitoring records, retention period for holding recorded information, security measures regarding storage of records and the location and effective times associated with how the monitoring will occur. • Employees should be informed of the consequences associated with any breach of the employer's policy. • Employers should ensure that their employees are able to exercise their right to access their own personal data collected in the course of employee monitoring, subject to the provisions of the PDPO. • Personal data should not be used for any purpose other than the purpose identified at the time of collection. • All practical steps should be taken to ensure that personal data held is protected against unauthorized access.
Bottom Line: The Guidelines are voluntary but provide good practical guidance on the steps that should be considered when monitoring in the workplace. The steps are similar to those recommended for workplace monitoring in the United States and in the European Union.		
Discussion: Generally speaking, the Guidelines require the employer's legitimate business interests to be balanced against employees' personal data privacy rights. To do this, the company should: (a) assess the risks that employee monitoring seeks to manage and the intrusiveness of the		

proposed monitoring techniques; (b) consider alternatives to employee monitoring that may be equally effective and practical in their application, yet less intrusive; and (c) document the reasons why monitoring is required. The assessment process for Hong Kong is similar to the impact assessment required in the United Kingdom.

India

General Privacy Laws	Personal Data Protection Laws	Workplace Privacy Laws
• The Constitution of 1950[70] does not specifically recognize the right to privacy. In 1964, however, the Supreme Court of India noted that there is a right of privacy implicit in the Constitution, which provides: "No person shall be deprived of his life or personal liberty except according to procedure established by law."[71] ▪ Indian law recognizes a general right of privacy; however, there is no general law regarding data privacy. ▪ In *Kharak Singh v. State of Uttar Pradesh,* the Supreme Court of India held that the right to privacy was an "essential ingredient of personal liberty" which is "a right to be free from restrictions or encroachments".	• India has no personal data protection laws or regulations. In 2000, the Indian Information Technology Act went into effect. This law makes punishable cyber crimes like hacking, damage to computer source code, and breaches of confidentiality and privacy. This law is unlikely to be applied to workplace monitoring, as it has no direct application to such monitoring. Instead, the Act is intended to provide a comprehensive regulatory environment for electronic commerce. The Act has no provision for the protection of personal data. • Over the last four or five years, news media have reported that India is considering legislation to provide safeguards to ensure data privacy protection in India.[72] • In June 2005, India's Prime Minister was quoted as requesting an amendment to the Indian IT Act to ensure any secrecy breach or illegal transfer of	• India has no legislation or regulations concerning monitoring in the workplace. • Due to growing concerns about employee theft of data and/or misuse of information, there has been an effort to curb employee fraud. In the BPO sector, a central employee database has been created by the National Association of Software and Service Companies (NASSCOM).[74] This registry endeavors to house updated information on employees working in the IT and BPO sector. The media has reported that this employees in the IT and BPO industries will be required to join this registry.[75]

[70] Indian Constitution, *available at* http://indiacode.nic.in/coiweb/welcome.html.
[71] Kharak Singh v. State of UP, (1964) 1 SCR 332; *see* R.C. Jain, National Human Rights Commission, India, Indian Supreme Court on Right to Privacy, July 1997, *cited in* Privacy & Human Rights, p. 568.
[72] *See* Stephanie Overby, *India to Adopt Privacy Rules,* CIO Magazine (September 1, 2003) *available at* http://www.cio.com/archive/090103/tl_data.html.

▪ In *Gobind v. State of Madhya Pradesh*, the Indian Supreme Court recognized a right to privacy derived from the constitutional rights to free speech, to personal liberty, and to move freely within the country.	commercial or privileged information would be punishable under the law. [73] India is considering such legislation in response to growing concerns in the European Union, the United States and elsewhere that the lack of such laws in India will hinder its ability to continue to serve as an outsourcing center for Western companies.	

Bottom Line: There are no laws or regulations governing workplace monitoring in India. The current business climate makes it likely that India will allow reasonable workplace monitoring even if privacy laws were to be enacted. Employers should consider providing notice; limiting monitoring to what is reasonable to protect the employer's interests and ensuring appropriate use and safeguarding of personal information obtained during monitoring. Employers should also consider providing employees with a statement regarding the consequences for failing to comply with policies and guidelines that are detected by monitoring.

Discussion: Continued pressure from the European Union has lead NASSCOM and other industry leaders to consider the adoption of formal privacy assurances in India. This assurance may take the form of a "Safe Harbor" agreement similar to the US and EU privacy framework. NASSCOM has also identified state-specific data privacy laws with which Indian regulations must comply, including the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, and California's identity protection law, SB 1386.[76]

All of these efforts are aimed at protecting the security of information that is being processed in India. To date, there has been little or no reported effort to pass legislation that would limit the ability of an employer to conduct reasonable workplace monitoring.

Indonesia

General Privacy Laws	Personal Data Protection Laws	Workplace Privacy Laws
• No constitutional or other legal protections related to personal data privacy.	• No personal data protection laws have been enacted.	• No workplace privacy laws, regulations or guidelines have been enacted.

[73] *See* Dinesh C. Sharma, *India to Tighten Data Protection Laws,* CNET News (June 29, 2005), *available at* http://news.com.com/India+to+tighten+data+protection+laws/2100-1029_3-5768412.html.
[74] *See,* National Skills Registry, *available at* https://nationalskillsregistry.com/nasscom/pageflows/itp/itpRegistration/begin.do
[75] *See,* Mark Ballard, *Indian Employee Database to be Mandatory*, The Register (May 15, 2006), *available at* OUT-LAW News, http://www.out-law.com/page-6921.
[76] *See* Privacy & Human Rights, p. 570, *citing* NASSCOM, "Indian Privacy Law," (2002) *available at* http://www.nasscom.in/artdisplay.asp?cat_id=652.

Bottom Line: There are no laws or regulations governing workplace monitoring in Indonesia.

Discussion: Indonesia is a participant in the APEC Privacy Framework negotiations. Although not currently required under Indonesian law, companies wishing to conduct workplace monitoring in Indonesia should consider providing notice to its employees.

Japan

General Privacy Laws	Personal Data Protection Laws	Workplace Privacy Laws

• Article 13 of the Japanese Constitution provides that "the right to life, liberty, and the pursuit of happiness shall . . . be the supreme consideration in legislation and in other government affairs."[77]
 	
• In 1963, the Japanese Supreme Court first recognized a substantial right to privacy based on Article 13. Court precedent has established a general right to privacy.[78]
	• On May 30, 2003, the Act Concerning the Protection of Personal Information (also called the **Personal Information Protection Act**) ('**PIPA**') was enacted after almost five years of debate in the *Diet* (the Japanese Parliament). The Act has an important exemption from its coverage: companies that hold personal data relating to 5,000 people or less and ordinary private use of personal information are exempt from the requirements of the law.
	
	• PIPA has two main parts:
	
	  • *Basic Ideals and Principles:* This part covers both the public and private sector and was created as a guideline for the framework for future privacy protections.
	
	  • *General Provisions:* Sets up guidelines for the protection of personal information in the private sector, outlining how companies must handle
		• There are currently no laws or regulations regarding workplace monitoring in Japan.
		
		• Companies wishing to monitor in Japan should look at the METI Guidelines. The guidelines provide that an employer should: (1) specify the purposes of monitoring; (2) create a privacy policy that incorporates specifics relating to monitoring; (3) Designate a person responsible for monitoring; and (4) Perform audits and confirm that monitoring is being conducted fairly.
		
		• Culturally, workplace monitoring has not been as prevalent in Japan as in the United States, Britain and other trading partners.

[77] Constitution of Japan, November 3, 1946. English translation *available at* http://www.solon.org/Constitutions/Japan/English/english-Constitution.html.
[78] *See,* Privacy & Human Rights, p. 620.
[79] The Act for Protection of Personal Data Held by Administrative Organs of 2003, Articles 53-55. English translation *available at* http://www.solon.org/Constitutions/Japan/English/english-Constitution.html.
[80] The Cabinet Office, Guidelines for Personal Information Protection, English translation available at http://www5.cao.go.jp/seikatsu/kojin/index_en.html.

	personal data. • PIPA adopts a self-regulatory approach to managing privacy in the public sector and allows agency ministers to mediate complain settlement regarding personal data usage disputes. Failure to abide by a minister's decision could result in prison terms or fines. Ministers' authority does not extend to information provided by the media. • Four personal information protection bills were enacted along with PIPA and cover: private business, government organizations and independent administrative agencies. [79] • The Cabinet Office directed each Ministry to create its own guidelines concerning personal information protection. Each Ministry has published individual guidelines aimed at regulating use of personal information in the private sector.[80] • Various Japanese ministries have issued guidelines on the use of personal information pursuant to the Law on the Protection of Personal Information. In the last three years since the Act went into effect, Japanese ministries have developed new guidelines and amended existing guidelines regarding the protection of personal information. The activities of a majority of businesses are covered by the guidelines promulgated by one of the following agencies: the Ministry of Economy, Trade and Industry (METI); the Ministry of Health, Labor and Welfare, the Financial	• Private surveillance in the workplace is on the rise in Japan. The Japanese Institute of Labor reports that 35% of Japanese companies are monitoring their employees' email and Web use, citing fear of viruses, sexual harassment and other concerns. [81] • According to a 2006 survey of 139 companies conducted by the Institute of Labor Administration, 17.4% of employers monitor their employees' incoming and outgoing emails, and 42% keep a record of the emails.[82] • On September 13, 2004, the Tokyo District court decided a case on the investigation of computer use of employees by employers. The court stated: "(1) whether or not the employers' act is an invasion of privacy rights of employees that goes against public policy depends on whether, balanced against the drawbacks suffered by the employees, the purpose or manner of the investigation goes beyond the bounds of socially acceptable limits." (2) If there are acts that violate the corporate order, employers may investigate the factual relationships

[81] "*35% of Companies Monitor Online Browsing, Email by Employees,* Japan Today (May 14, 2002), *available at* http://www.japantoday.com/e/?content=news&cate=4&id=215446, *cited in* Privacy & Human Rights, p. 629.
[82] "*The Boss May be Monitoring Your Emails,"* Japan Today (June 9, 2006), *available at* http://www.japantoday.com/jp/shukan/345 .
[83] Case Number: 26741 (wa) 2003.

	Services Agency, the Ministry of Internal Affairs and communications and the Ministry of Land. As of September 1, 2007, these ministries have established 35 sets of guidelines, covering 22 business areas.	regarding the content, manner and degree of the violating acts, and employees must cooperate with the employer pursuant to their employment contract, but it is sufficient for such cooperation to be within the range necessary and rational in order for the employer to smoothly conduct operations."[83]

Bottom Line: Companies wishing to monitor employees in Japan should adopt a privacy policy specifically stating that monitoring will take place. Monitoring should be balanced against the employees' expectation of privacy. Where the private use of e-mail, for example, is prohibited by company rules and those rules are actually implemented, employees' expectation of privacy is low, so monitoring without giving notice is usually acceptable provided there is a rational reason to monitor and a person is clearly specified as responsible for monitoring.

Monitoring should be balanced against the employee's expectation of privacy. This means that notifying employees clearly and publicly in advance of network, Internet or e-mail monitoring is absolutely essential. An employer infringes privacy rights when the purpose, method, and manner of monitoring, when balanced against the privacy intrusion suffered by the person being monitored, would be socially inappropriate.[84]

Discussion: Similar to Hong Kong, the Japanese Government has published guidelines on the processing of personal information. Several provisions of these published guidelines relate to monitoring. These supplement the Law on the Protection of Personal Information 2005 which does not directly relate to employee monitoring. The Guidelines provide that an employer should: (1) specify the purposes of monitoring and incorporate them into its employee privacy policy; (2) designate the person responsible for monitoring and the authority of that person; and (3) perform audits and confirm that monitoring is being conducted appropriately.

Malaysia

General Privacy Laws	Personal Data Protection Laws	Workplace Privacy Laws
• The Constitution of Malaysia does not specifically recognize a right to privacy. [85]	• There is no personal data protection law in Malaysia.	• There are no laws or regulations regarding workplace monitoring.

[84] Tokyo District court (wa) 12081 of 2000, *cited in* Morrison & Forrester, Employee Privacy: Guide to U.S. and International Law (2007), at p. 3-49.

	• The Personal Data Protection Bill of 1998 was expected to have been enacted in 2004, but has been repeatedly delayed. The bill, if enacted, would establish common guidelines to regulate the handling and use of personal data by any person or organization. It would set out the following data protection principles: notice, choice, disclosure, security, data integrity, access, and enforcement. [86] • The proposed legislation does not attempt to prohibit the collection, holding, processing or use of personal data, nor does it deal with access.[87]	

Bottom Line: There are no laws or regulations governing workplace monitoring in Malaysia.

Discussion: Malaysia is a participant in the APEC Privacy Framework negotiations. Although not currently required under Indonesian law, companies wishing to conduct workplace monitoring in Indonesia should consider providing notice to its employee.

New Zealand

General Privacy Laws	Personal Data Protection Laws	Workplace Privacy Laws
• The New Zealand Court of Appeals has interpreted Article 21 of the New Zealand Bill of Rights Act of 1990 as protecting the right to privacy. Article 21 provides: "Everyone has the right to be secure against unreasonable search or seizure, whether of the	• New Zealand's Privacy Act of 1993[89] • Regulates the collection, use and dissemination of personal information in both public and private sectors. • Grants individuals the right to have access to	• Employers must obtain the consent of the employees and have the appropriate policies in place for such monitoring. Otherwise, any workplace monitoring must be done in accordance with the Privacy Act of 1993.

[85] Ultra Demision v. Kook Wei Kuan, 5 CLJ 285 (2004) *available at* http://www.cljlaw.com/ (Laws of Malaysia Database, subscription service only), *cited in* Privacy & Human Rights, p. 700.
[86] *See "Proposals for a Personal Data Law,"* World Data Protection Report, November 2003.
[87] Privacy & Human Rights, p. 710.

person, property, or correspondence or otherwise."[88]	their personally identifiable information held by any agency. • Creates 12 "Information Privacy Principles" based on the 1980 Organization of Economic and Cooperation Development (OECD) and the information privacy principles in Australia's Privacy Act of 1988. • Authority concerning data protection rights is granted to the Office of the Privacy Commissioner, an independent oversight authority that was created in 1991 as part of the Privacy commissioner Act. [90]	• It has been widely reported by commentators in New Zealand that it is widely accepted for employers to monitor employees' email sent from work computers.[91] • The New Zealand Privacy Commissioner has provided a "how-to-guide" for employers and gives the following steps for conducting workplace monitoring:[92] • Determine legitimate justification for monitoring. • Develop a draft policy setting out why monitoring will take place and when it will occur (*e.g.,* on a regular basis, only on suspicion that something inappropriate has happened, etc.). • Circulate the draft policy to employees and discuss it with them or their union. • Remind everyone why monitoring

[88] New Zealand Bill of Rights Act of 1990, *available at* http://www.oefre.unibe.ch/law/icl/nz01000_.html (last visited February 11, 2007).
[89] *Available at* http://www.knowledge-basket.co.nz/privacy/legislation/1993028/toc.html (last visited February 11, 2007).
[90] *See* Privacy Commissioner's Website *at* http://www.privacy.org.nz/home.php (last visited February 11, 2007).
[91] *See* Kelly, Andrew, "*NZ Bosses Free to Read Staff E-Mails,* The Dominion Post (Wellington), April 10, 2004, at 5.
[92] *See* http://www.privacy.org.nz/how-to-comply/information-for-employers (last visited February 11, 2007).
[93] *See* Bell Gully, "Wayward Emailers Get the Message" FindLaw Articles (March 2001), available at *http://72.14.203.104/search?q=cache:-4VwuTGDFGQJ:www.findlaw.com/12international/countries/nz/articles/334.html+new+zealand+monitor+employee+email&hl=en&gl=us&ct=clnk&cd=1* . The employees were being monitored for unrelated confidentiality issues. The author warns employers to be wary of using private information gathered during unrelated monitoring.

		is necessary. • Listen to feedback. • Make any necessary adjustment to the policy and issue it. • The Employment Court was unsympathetic to the claims by three employees who were fired for exchanging offensive emails. In Clarke v. Attorney General [1997] ERNZ 600. [93] • Under the Privacy Act, employers may undertake monitoring in the workplace under certain conditions: there must be a lawful purpose and the information collected must be necessary to achieve that purpose. Employers must ensure that unfair or reasonably intrusive means are not used during monitoring. • Covert monitoring in the workplace is permitted if open monitoring would prejudice the purpose for which emails are to be monitored. In such cases, employee consent is not required
Bottom Line: Adopt a privacy policy specifically stating that monitoring will take place and that employees have no reasonable expectation of privacy with respect to communications on the company's network or equipment. State why monitoring is taking place.		
Discussion: As in the United States, notice to employees is a necessary and sufficient requirement for monitoring under the Privacy Act of 1993. If employees have received notice, then the expectation of privacy has been removed. Employee e-mail can be monitored without providing		

notice to the employee if providing notice would prejudice the purpose for monitoring. The Privacy Act allows the covert collection of information in those circumstances involving potentially unlawful behavior as it recognizes that giving notice in relation to an investigation may thwart the purpose of the investigation.

Pakistan

General Privacy Laws	Personal Data Protection Laws	Workplace Privacy Laws
• There is no constitutional right to privacy.	• Pakistan has not enacted a personal data protection law.	• Pakistan has not enacted workplace privacy laws.

Bottom Line: There are no laws or regulations governing workplace monitoring in Pakistan.

Discussion: Pakistan is not a member of APEC nor is it currently involved in the development of the Privacy Framework. Nevertheless, it is recommended that you adopt a privacy policy notifying employees that monitoring will take place.

Philippines

General Privacy Laws	Personal Data Protection Laws	Workplace Privacy Laws
• Section 3(1) of the Constitution states that "privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law."	• The Philippines does not currently have a data protection law; however, there are two pieces of pending legislation that would protect data privacy in both the public and private sectors. The two pieces of proposed legislation are: the Government Data Privacy Protection Act of 2007. The Data Privacy Protection bill seeks to ensure the security of data in the government's possession. The Government Data Privacy Protection is pending review in committee. • Administrative Order No. 8 seeks to cover the private sector data handling practices.	• The Philippines does not have a law specifically regulating workplace activity.

	• Administrative Order No. 8 establishes principles for data processing, including the following: (1) data must be collected for specified and legitimate purposes determined before collecting the personal data and processed in compliance with those purposes; (2) personal data must be processed accurately, fairly and lawfully; (3) accurate and, when appropriate, up-to-date; (4) Inaccurate or incomplete data must be corrected, supplemented or destroyed and (5) kept in a form that allows identification of the data subject, and for no longer than it is necessary for the purposes for which it was collected. • Administrative Order allows the processing of personal data in only four conditions: (1) When the data subject unambiguously authorizes the processing; (2) the personal data processing is the result of the data subject contractual obligation; (3) where the data processing is "vitally important to protect the data subject, including life and health; and (4) when the data controller requires to process personal data in compliance with his or her lawful obligation and only to the extent authorized by the parties. • Section 8 of Guideline 8 addresses the issue of Security of Data. In the Philippines, data controllers must implement organizational and technical means to assure protection of personal data from destruction, alteration or disclosure. • Article 26 of the Civil Code states that "every person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons. The following and similar acts, though they may not constitute a criminal offense, shall produce a cause of action for damages, prevention and other relief:	

	(1) Prying into the privacy of another's residence; (2) Meddling with or disturbing the private life or family relations of another; (3) Intriguing to cause another to be alienated from his friends; (4) Vexing or humiliating another on account of his religious beliefs, lowly station in life, place or birth, physical defect, or other personal condition." • Article 32(1) of the Civil Code states that "any public officer or employee, or any private individual, who directly or indirectly obstructs, defeats, violates or in any manner impedes or impairs the privacy of communication and correspondence shall be liable to the latter for damages."	

Bottom Line: Adopt a privacy policy or technology use policy notifying employees that workplace communications will be monitored. State the reasons for monitoring and limit the use of information gathered during monitoring to the stated uses.

Discussion: The Philippines is a member of APEC and is working on the APEC Privacy Framework. If your company will conduct workplace monitoring in the Philippines, consider following the best practices recommended by the Privacy Framework and the general requirements of Administrative Order No. 8.

Singapore

General Privacy Laws	Personal Data Protection Laws	Workplace Privacy Laws
• The Singapore Constitution does not contain an explicit right to privacy.[94] However, personal information has been found to be protected from disclosure in some instances	• Singapore has no overarching legislation for the protection of personal data. The Ministry of Finance has a small department handling privacy and data protection matters, primarily under banking specific legislation.	• Employer monitoring of employee phone calls, e-mails and Internet usage is permissible under Singapore law. Under Singapore property law, workplace e-mail, telephone, and

[94] *See,* Constitution of the Republic of Singapore. English translation is *available at* http://www.oefre.unibe.ch/law/icl/sn00000_.html.

according to Singapore's high court.[95]	• Under Singapore's common law, confidential information may be protected under a duty of confidence, which usually arises under a contractual obligation. • Personal information is also protected under sector-specific laws such as the Banking Act,[96] Statistics Act,[97] the Official Secrets Act, [98] and the Statutory Bodies and Government Companies (Protection of Secrecy Act).[99] None of these regulate workplace monitoring, however. • In February 2002, the National Internet Advisory Committee of Singapore released a "Model Data Protection Code for the Private Sector." The Draft Code is modeled on the principles previously adopted by the EU Data Protection Directive (1995), the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the 1996 Canadian Standards Association Model Code for the Protection of Personal Information.[100] The Model Data Protection Code is voluntary and does not specifically address issues of workplace monitoring.	computer equipment is the property of the employer. As a result, if an employee loses his job based on communications at work, he has no ground for defense based on an invasion of privacy.[101]
Bottom Line: Adopt a privacy policy or technology use policy notifying employees that workplace communications will be monitored. State the reasons for monitoring and limit the use of information gathered during monitoring to the stated uses.		

[95] *See* Privacy International, *The Republic of Singapore* (November 16, 2004), *available at* http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83777.
[96] Banking Act 2003, *available at* http://www.mas.gov.sg/masmcm/bin/pt1Banks.htm.
[97] Singapore Statistics Act, Ch. 317 (1999 Rev. Ed.), *available at* http://statutes.agc.gov.sg/non_version/cgi-bin/cgi_retrieve.pl?actno=REVED-317.
[98] Singapore Official Secrets Act, *available at* http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_getdata.pl?actno=1935-REVED-213&doctitle=OFFICIAL%20SECRETS%20ACT%0A&date=latest&method=whole&sl=1.
[99] *See* Singapore Government, Policies & Regulation, *at* http://www.ida.gov.sg/Policies%20and%20Regulation/20060627155443.aspx.
[100] *See* Vivianne Jabbour, *The Draft Model Data Protection Code in Singapore,* BNA World Data Protection Report (August 2002).
[101] See Privacy International Country Reports, Republic of Singapore available at http://www.privacyinternational.org/survey/phr2003/countries/singapore.htm#ftnref2237.

Discussion: Singapore is a member of APEC and is working on the APEC Privacy Framework. If your company will conduct workplace monitoring in Singapore, consider following the best practices recommended by the Privacy Framework. While this is not currently required, it will help avoid misunderstandings and should prepare your company for any future legislation in Singapore.

Republic of South Korea

General Privacy Laws	Personal Data Protection Laws	Workplace Privacy Laws
• The Constitution of the Republic of Korea recognizes the right to privacy, including the protection of secrecy and liberty of private life.[102] • Article 16 of the Constitution states that all citizens are free from intrusion into their residence and search of a residence requires a search warrant. • Article 17 states that no citizen's privacy should be infringed.	• In 2000, South Korea introduced an Act on Promotion of Information and Communications network Utilization and Information Protection (**Information Protection Act**).[103] The Information Protection Act sets out guidelines for personal data protection in the private sector. • The Information Protection Act applies to "providers of information and communications services" and restricts the gathering of personal information. Article 22 *et seq.* requires providers to obtain consent of a "user" before personal information is gathered.	• In Korea, the monitoring of workplace e-mails of employees is covered by the Act on Promotion of Information and Communications Network Utilization and Information Protection (APICNU) and the Protection of Communications Secret Law of 1993 (the Secrecy Act). • Under Article 48 of APICNU, any person is prohibited from infiltrating information and communications networks without any justifiable access right or beyond the permitted access right. • Unless notice and express consent are obtained from employees, monitoring of employee e-mails is likely to be viewed as a violation of Article 48 of APICNU. Even if the computers are owned by the employer, without notice and consent

[102] Constitution of the Republic of Korea (1948). English translation *available at* http://www.isop.ucla.edu/eas/documents/korea-constit.htm .
[103] English translation *available at* http://www.worldlii.org/int/other/PrivLRes/2005/2.html.

		of the employer, monitoring of e-mails is likely to be deemed to have gone beyond the permitted access right and to be in violation of Article 48. • Article 3 of the Secrecy Act prohibits any person from censoring any mail, wiretapping any telecommunications, providing communication confirmation data, or recording or listening to conversations between others that are not made public. E-mails are considered to be "telecommunications" under the Secrecy Acts. • Monitoring of e-mails under the Secrecy Act is permitted only if (1) the sender and receiver consent; (2) monitoring is protected under the Secrecy Act; or (3) monitoring is done pursuant to the Criminal Procedure or Military Court Act. Therefore, unless employees provide the employer with consent to monitor their e-mails, the employer will likely be in violation of Article 3 of the Secrecy Act. The consent of the sender of the e-mail received by the employee will likely to be presumed in the case of work e-mails, as these e-mails are usually viewed as emails exchanged on behalf of the employer.

[104] *See* Miriam Wugmeister, Ann Bevitt, Peter J. Edling, *"Employee Monitoring: Highlighting the Issues"* Morrison Foerster Legal Updates & News (August 2005) *available at* http://www.mofo.com/news/updates/files/update02051.html.

		• Employers should also be aware that reading of the e-mails requires the breaking of a security device (e.g., a password), this may be a violation of Article 316 of the Criminal Code. • The **Information Protection Act** could apply to employers who provide communications services.[104] In light of this, employers should: o Clearly inform their employees of the scope of monitoring and how it is carried out. o Advise employees to store their personal e-mails separately or not to use company facilities for personal emails. o Obtain employee consent before monitoring.
Bottom Line: Notice of monitoring alone, even if the company has a legitimate reason to monitor, is insufficient. An employee must also give his express consent. Accordingly, adopt an appropriate privacy or technology use policy, state the reasons for monitoring and obtain employee written consent and an acknowledgement that he understands the policy and reasons for monitoring. Additionally, if information will be transferred outside of Korea, notice and consent should be obtained.		
Discussion: Korea's laws are closer to those of the EU than many of the other countries of the APAC region. Before monitoring takes place, you should: (1) clearly inform your employees of the scope of monitoring and how it is carried out; (2) advise employees to store their personal e-mails separately; and (3) obtain explicit consent before monitoring.		

Taiwan

General Privacy Laws	Personal Data Protection Laws	Workplace Privacy Laws
• Article 12 of the Republic of China Constitution of 1946 states that citizens should have freedom concerning correspondence.[105] • An infringement of the right to privacy may be subject to civil liabilities under the Civil Code. • Authorities on the country's legal system ask whether or not the employees had a reasonable expectation of privacy in order to determine if the monitoring were proper.	• Taiwan has had detailed data privacy legislation since 1995; however, this applies only to public sector entities. • The Computer-Processed Personal Data Protection Law of 1995 governs the collection and use of personally identifiable information by government agencies.	• Taiwan has no legislation specifically regulating workplace monitoring. • A district court case from 2003 adopted the "reasonable expectation" test for workplace monitoring. Under this test, companies can only monitor employee emails if they do not have a reasonable expectation of privacy of their work emails. The opinion of the district court judge was that the ability of an employer to monitor its employees' work e-mails depended on whether or not the employees had a reasonable expectation of privacy for their work e-mails. • Implied Consent: The court stated that an employer may announce its e-mail monitoring policy to the employees. If the employees do not object to such a policy, the employees should be deemed as having given implied consent. The district court also concluded that there are no other laws and regulations explicitly prohibiting employers from monitoring employees' work e-mails. • Statute Governing the Protection and

[105] Constitution of the Republic of China (1946). English translation *available at* http://www.oefre.unibe.ch/law/icl/tw00000_.html.

		Monitoring of Communications governs the interception and monitoring of private communications by the policy. Certain civil and criminal liabilities, however, apply to all persons. For employer to be exempt from liabilities under this law, he must obtain consent of employees and the employer's monitoring cannot be for illegal purpose. • The Criminal Code prohibits individuals from intercepting or monitoring "non-public" speeches or activities of others unless there is a legal justification.
Bottom Line: Publish a clear policy on workplace monitoring, advising employees that they have no expectation of privacy with respect to emails using the company computer equipment and that monitoring will take place. The employer should announce Work Rules that include a provision regarding the possibility of monitoring. In addition, the employer should, to the extent possible, obtain employee consent by including such a provision in employment contracts.		
Discussion: Taiwan has a similar approach to monitoring as New Zealand. Adopt a policy and provide specific notice to employees that monitoring will take place. Ensure that employees have no reasonable expectation of privacy in connection with their emails and other use of the company's network and computer equipment.		

Thailand

General Privacy Laws	Personal Data Protection Laws	Workplace Privacy Laws
• Thailand Constitution of 1997 includes rights to privacy and rights to government information.[106] Both of these rights, however, are qualified	• Thailand has no comprehensive data protection laws.	• Thailand has no legislation specifically regulating workplace monitoring.

[106] Constitution of the Kingdom of Thailand (1997). English translation *available at* http://www.parliament.go.th/files/library/b05-b.htm.

in the interests of society.		
Bottom Line: There are no laws or regulations governing workplace monitoring in Thailand.		
Discussion: Thailand is a participant in the APEC Privacy Framework. If your company will conduct workplace monitoring in Thailand, consider following the best practices recommended by the Privacy Framework. While this is not currently required, it will help avoid misunderstandings and should prepare your company for any future legislation in Thailand.		

Vietnam

General Privacy Laws	Personal Data Protection Laws	Workplace Privacy Laws
• Vietnam's constitution does not provide a right to privacy.[107]	• Vietnam has no comprehensive personal data protection laws.	• Vietnam has no legislation specifically regulating workplace monitoring.
Bottom Line: There are no laws or regulations governing workplace monitoring in Vietnam.		
Discussion: Vietnam is a participant in the APEC Privacy Framework. If your company will conduct workplace monitoring in Vietnam, consider following the best practices recommended by the Privacy Framework. While this is not currently required, it will help avoid misunderstandings and should prepare your company for any future legislation in Vietnam.		

[107] *See* Constitution of the Socialist Republic of Vietnam (1992). English translation *available at* http://www.oefre.unibe.ch/law/icl/vm00000_.html.

How Vontu Effectively Safeguards Employee Privacy

In developing its technology, Vontu clearly has given considerable thought to helping its customers effectively monitor the use of sensitive information while safeguarding employee privacy. Vontu's technology accomplishes this in a number of ways:

COMPLY WITH NOTICE AND POLICIES: Vontu enables companies to comply with their privacy notices and policies. Vontu does this through policy-based monitoring.

LEGITIMATE PURPOSES AND PROPORTIONALITY: Vontu ensures that data collected during monitoring is only used for legitimate purposes. Vontu enables companies to collect only data that violates policies, and then enables companies to ensure that only those individuals with a "need to know" have access to the collected data.

TARGETED MONITORING: The fair information practice principles and the principles set forth in the OECD and APEC guidelines require companies to collect data for legitimate purposes and then collect only such information that is proportional to the company's purpose for data monitoring. Vontu accomplishes this in several ways. First, Vontu safeguards employees' privacy by treating the sender's identity as "need-to-know." Second, Vontu collects only data that violates stated policy. And third, Vontu limits access to collected data to individuals who are approved to receive it.

DATA INTEGRITY/ACCURACY: Collecting information that does not violate policy or information on the wrong individuals increases a company's privacy risks. Vontu has greatly reduced these risks by keeping false positives near zero.

SECURITY: Vontu provides security for the data that is collected by providing secure communications of incident data. Additionally, Vontu provides for role-based access to incident information and a complete audit trail.

ENFORCEMENT: Vontu provides an audit trail for all information gathered during monitoring. Significantly, Vontu maintains the integrity of audits by logging changes to policies and all activities taken in response to an incident.

ONWARD TRANSFER: Vontu enables its customers to restrict the transfer of personal data, thereby reducing the risks under the EU Data Protection Directive or laws of individual countries that may limit the onward transfer of personal data.

ACCESS: Vontu's audit trail enables companies to easily provide individuals or worker representatives with access to specific information.

This section will examine some of Vontu's key functions that safeguard employee privacy while protecting against the loss of sensitive information.

Limits the Disclosure of Personal Information: "Need to Know"

Privacy laws and regulations apply to information that can be associated with a particular individual. If the information is anonymous or if the information is not otherwise tied to a particular individual, the risks of violating an employee's privacy rights are greatly reduced.

Vontu's Monitor detects confidential information before it leaves the network over e-mail, instant message or the Web. Vontu's Prevent stops confidential information from leaving the network and prevents internal security breaches before they occur. If a transaction is identified as a violation of the company's policies, it is cached and stored on the Vontu Monitor. This automatically triggers a transaction to Vontu Enforce by providing basic information about the policy violation. The identity of the sender, however, does not have to be disclosed. The identity of the sender can be restricted to those the company has determined have a legitimate "need to know." Vontu can also send a message to the sender that a policy violation has occurred.[108]

Vontu can also be configured to comply with the transborder data transfer restrictions of the EU, Australia or any other country that restricts transborder transfer. Vontu's Monitor and Enforce can be set up so that they reside in one location within a particular country. Accordingly, data collected during monitoring does not travel across national boundaries.

Legitimate Purpose and Proportionality: Policy-Based Monitoring and Focus on Specific Activities

The principles of legitimate purpose and proportionality provide that monitoring is justified only if it is necessary to protect the legitimate interests of the employer and the monitoring goes no further than is necessary to meet that need. A company usually discloses the legitimate purpose in documents such as a "Network Use" policy, an "Employee Privacy" or "Customer Data Privacy" policy.

Vontu automates policy enforcement options for notification, workflow, blocking, quarantine and encryption. Vontu allows users to define and deploy data security policies based on over fifty pre-built policy templates for protecting customer data, intellectual property and company confidential information.

The focus on specific activities and policy-based monitoring helps avoid additional compliance and privacy exposures. It enables a company to provide notice of exactly what is being monitored and what is being collected. Vontu's match highlighting gives the company a clear indication of why a communication generated an incident, saving time in the incident review process and ensuring that data collected is limited to that which violates policies.

Collects Only Data that Violates Policy

Vontu monitors data flowing across a network but **only** collects data if it violates company policy. This is a significant step in protecting employee's privacy rights. Whereas some monitoring technologies capture all data – even that which does not violate policy, Vontu does not. Some of

[108] Notice to the originator of the e-mail can play an important role in establishing notice under both US and the data privacy laws of other countries. This can be the event that alerts an employee that his or her communication has been recorded as an incident and, therefore, triggers any rights they may have to access the data collected about the violation.

Vontu's competitors enable companies to run queries against all of the captured data in an effort to find violators. This is a clear violation of the principle of proportionality and one that Vontu does not allow.

Data Accuracy and Integrity: Limits False Positives

Vontu's patent-pending technology accurately detects confidential data across all network protocols, content formats and business contexts. Accurately identifying information that violates policy is key in reducing false positives.

Vontu's Exact Data Matching delivers a high degree of accuracy on structured data. This is essential for protecting customer and employee data. Vontu's Indexed Document Matching creates "digital fingerprints" on unstructured content, enabling accuracy. And finally, Vontu's Described Content Matching uses keywords, lexicons, pattern matching (regular expression), file types, file sizes, sender, receiver and network protocol information to detect data loss incidents.

Security for Data Collected

Vontu has provided numerous features to safeguard the data that is gathered during monitoring. To begin with, the information on violations is revealed to first responders or analysts through a secure visual display. In order to protect this information during transmission, Vontu uses a secured communication channel or encrypts the information being sent. Vontu's stored (cached) documents and summary reports reside within a company's secure corporate LAN and the information is not transferred to outside parties.

Vontu also allows a customer to determine who should see specific information on incidents. The role-based access controls are important to minimize risks of the improper use of sensitive information. A customer can limit access to sensitive information or sender identity to departmental supervisors or others who should have access to such information.

Access and Enforcement: Comprehensive Audit Trail

One significant aspect of privacy protection is ensuring that an audit trail is kept of the collection and use of information. Additionally, the audit trail should keep complete records on any changes to policies as well as steps taken as a result of the incident. Vontu keeps detailed logs and accurately timestamps and records the information necessary to resolve disputes. Further, Vontu preserves evidence that may be needed for later use in the event of intentional violations.

Vontu keeps complete data on all incidents for purposes of an audit trail. Significantly, Vontu enables customers search historical data based on sender, policy, recipient and other relevant factors. This can be adjusted to comply with the EU's restrictions on how long personally identifiable data can be retained.

Onward Transfer: Limiting the Need to Transfer Data

Vontu helps its customer reduce risks from the unauthorized or inappropriate transfer to personal data collected during monitoring. Under the laws of the EU, for example, the unauthorized transfer of personal data on residents of the EU to the US – even within the same company – can be a violation of law. Sanctions for such unauthorized transfer can include injunctions, monetary

fines against the company *and* the individual employees who transferred the data and criminal penalties.

Vontu enables it customers to restrict the transfer of personal information. If data should not be transferred outside of a particular country, for example, Vontu can be set up so that all components reside in one location within that country and data will not move across national boundaries. Vontu also enables its customer to de-identify incident data so that personal information is not being transferred across national boundaries. These features are particularly important for U.S-based companies that have offices or affiliated entities located in the EU or other jurisdictions that restrict transborder transfers.

Grading Vontu for Effective Management of Workplace Privacy

At the outset of this paper, it was noted that effective management of workplace privacy issues requires a multi-faceted approach. Companies must educate themselves on the requirements of both US and Asia, the Pacific and Japanese laws governing workplace monitoring. Companies must also put in place effective policies and procedures to regulate monitoring and to reduce employees' expectation of privacy for workplace communications. One important element is the adoption of the Vontu solutions that will enable companies to comply with their policies, protect their sensitive information while safeguarding employee privacy. Vontu is such a technology and provides reasonable steps to protect and secure data that is gathered as a result of targeted monitoring. Vontu receives high marks for its effort to provide its customers with effective tools for safeguarding employee privacy while providing effective monitoring.

Table 1 below provides a scorecard to determine how Vontu meets the fundamental privacy principles underlying workplace monitoring. It contains a listing of the basic fair information practice principles of the United States and the relevant principles from the APEC Privacy Framework as they relate to workplace monitoring.

Table 1

Monitoring Requirements Under APEC Privacy Framework

Requirement	How Vontu Meets Requirement	Yes/No
Preventing Harm: Remedies should be proportionate to the likelihood and severity of any harm threatened by the collection or use of personal information.	Vontu's policy-based monitoring allows companies to ensure that only non-compliant data is collected. This allows a company to set its policies and then feel comfortable that the monitoring is being limited to that related to the company's policies. Vontu Discover can automatically enforce data security policies by relocating exposed and confidential data to a quarantine area or encrypted file server and notifying owners.	**Yes**
Notice: Companies must notify individuals about the purposes for which they collect and use personally	Companies must notify individuals about the purposes for which they collect and use information. Although Vontu 7.0 does not provide the actual notice, companies can	**Yes**

Table 1		
Monitoring Requirements Under APEC Privacy Framework		
Requirement	**How Vontu Meets Requirement**	**Yes/No**
identifiable information. Notice may also require information on who is collecting the data, how it is being collected, where it will be processed and when.	use Vontu to ensure that monitoring takes place in compliance with the stated purposes in the notice and, therefore, that the information in the notice is accurate. Companies most often get into trouble for stating one thing in their privacy notice and then doing something different in practice. The ability to use technology to aid in complying with a company's privacy policies is an important step in reducing privacy risks.	
Collection Limitation: Personal information should be collected by lawful and fair means. Information that is collected should be limited to information that is relevant to the purposes of collection.	Vontu provides pre-built templates to assist customers in complying with privacy laws and best practices. Vontu provides content aware policy-based monitoring to ensure that monitoring and data gathering only target information that violates the company's policies. These are important steps in ensuring that a company is conducting monitoring for legitimate purposes and collecting only relevant information.	**Yes**
Security Safeguards: The information gathered must be protected from unauthorized use, access, loss, alteration or destruction.	Vontu allows role-based access to incident information. Vontu provides a complete audit trail of incident workflow. Finally, Vontu provides secure communication of the incident data. Vontu Discover can automatically enforce data security policies by relocating exposed and confidential data to a quarantine area or encrypted file server and notifying owners.	**Yes**
Access and Correction: Individuals must be given reasonable access to all personal information held about them.	Vontu's audit trail maintains a complete record if an incident workflow and all information related to the message that violated policy. Companies can easily provide employees or works council representatives with access to information on the violation.	**Yes**
Data Integrity: Steps must be taken to ensure that data is accurate and relevant for the purpose(s) for which it was collected.	Personal information must be relevant for the purposes for which it is to be used. Vontu's accuracy in monitoring data and its content aware, policy-based monitoring help ensure that the data gathered is relevant for the stated purposes.	**Yes**

Table 1		
Monitoring Requirements Under APEC Privacy Framework		
Requirement	**How Vontu Meets Requirement**	**Yes/No**
Enforcement: Measures must be put in place to ensure that data is used appropriately and that the policies regarding the use of the data are enforced. Effective enforcement includes an audit trail of how data is used to ensure that individuals who violate privacy policies are dealt with appropriately.	While Vontu 8.0 will not provide the actual dispute resolution mechanism, it does provide the audit trail and records necessary for an effective dispute resolution program. Since all information related to an incident is captured and logged, along with changes to the relevant policies, employees or works council representatives can have confidence that the information is accurate and that it has not been "manufactured." If information has been inappropriately used, the Vontu audit trail will enable companies to appropriately deal with the individuals who have violated the relevant policies.	**Yes**

Table 1 provides only a starting point for you to consider before monitoring employees within the APAC region. Because the laws and regulations vary from country to country, it is important that you understand the laws related to each country where you are doing business. It is also very important to understand the cultural and historical perspectives of each country regarding monitoring and privacy. For some countries in the APAC region, privacy is viewed as an important right that must be protected. In addition, it is important that you understand the technology that you will use to conduct monitoring, as its effectiveness and reliability can have an impact on the privacy risks you may be facing. Monitoring technology that provides safeguards to protect privacy rights of employees is an important step in managing privacy risks.

How to Get Started with Vontu

Vontu's team of Data Loss Prevention experts will work with you to understand your unique data security requirements, priorities, and share insight into our industry's best practices. Contact Vontu to get started at +1.415.464.8100 or email info@vontu.com.

About Vontu

Vontu is the leading provider of Data Loss Prevention solutions that protect data anywhere – at rest, in motion or at the endpoint. By reducing the risk of data loss, Vontu helps organizations ensure public confidence, demonstrate compliance and maintain competitive advantage. Vontu customers include many of the world's largest and most data-driven enterprises and government agencies. Vontu has received numerous awards, including IDG's InfoWorld Technology of the Year Award for "Best Data Leak Prevention," as well as SC Magazine's 2006 U.S. Excellence Award for "Best Enterprise Security solution" and global Award for Best New Security Solution." For more information, please visit www.vontu.com.

Conclusion

Monitoring has become an important part of the steps that companies must consider in order to protect their sensitive information. As discussed throughout this paper, monitoring can be used to protect the company's intellectual property as well as to protect against the leaking of customer or employee data. In order to effectively manage the risks related to the loss of sensitive data – without creating new risks by improper monitoring, companies must implement a multi-faceted program. Such a program must address the complex privacy and data protection laws of the US and the EU. An important part of any such program is the implementation of technology that provides management with an effective tool in dealing with workplace monitoring and privacy issues. Vontu technology is such a technology that should be considered by companies with international operations.

About the Author

Gary Clayton is the founder and CEO of Privacy Compliance Group, Inc., a leading privacy and data protection consulting and technology company. Privacy Compliance Group works with organizations to develop and implement effective privacy compliance programs and to develop practices and policies to comply with privacy laws around the globe.

Gary Clayton has worked with leading companies around the world and with numerous agencies of the US Government, including the Department of Homeland Security, the Department of Transportation, the General Accounting Office and the Federal Trade Commission. He has extensive experience in all aspects of privacy and has been actively involved in working with clients in over 55 countries. Mr. Clayton has worked in the EU and assisted the US Department of Commerce in negotiations with the EU on the Safe Harbor agreement and the Department of Homeland Security in negotiations regarding access to passenger data.

Mr. Clayton is an attorney who is admitted to practice in Washington, D.C., Texas and Louisiana. He has lived and studied in Europe where he received an advanced law degree (LLM) in European and International Law from the University of Exeter, England. He has also attended the law school at the university in Grenoble, France. He is a frequent author and speaker on global privacy and data protection issues. He can be contacted at gclayton@privacycg.com.

^Back to Table of Contents^