Privacy Year in Review: Canada's Personal Information and Protection and Electronic Documents Act and Japan's Personal Information Protection Act

ASIM Z. HAQUE & MATHIEW H. LE*

ABSTRACT

Of the many international laws affecting privacy rights that developed during 2004, two of the most important are Canada's Personal Information and Protection and Electronic Documents Act ("PIPEDA") and Japan's Personal Information Protection Act. The legal and statutory history of both acts is reviewed. Additionally, this article analyzes the meanings of the various terms and conditions within the two acts. Due to the recent passage in 2003 of the Personal Information Protection Act, an in-depth discussion of its language and requirements is provided. The Canadian case, Eastmond v. Canadian Pacific Railway, is used to illustrate the emerging requirements and intricacies of PIPEDA. Its analysis includes a discussion of jurisdiction, the de novo standard of review, and consent under PIPEDA. Also included in the analysis of PIPEDA is a discussion of the four-part test used to determine whether the purposes for collecting personal information are those a reasonable person would consider appropriate. Analysis of the Personal Information Protection Act includes looking at the future impacts and interpretations of the act. In particular, this article discusses the possible impacts the act may have on United States businesses that do business in Japan. Finally, the Personal Information Protection Act is viewed in comparison with United States and European Union privacy regulations and legislation.

I. INTRODUCTION

Protection of personal information is not only an American concern but is indeed an international one. Citizens living in countries with even the most modest economies have concerns about their privacy and whether their personal information is being misused. Two countries that have recently taken measures to protect their citizenry's personal information are Canada and Japan. In 2000, Canada enacted

---

* Asim Haque and Mathiew Le are both candidates for juris doctor at The Ohio State University Moritz College of Law, class of 2006. Asim Haque also holds a B.A. with a double major in chemistry and political science from Case Western Reserve University. Mathiew Le has a B.A. in microbiology from the University of Texas at Austin.

the Personal Information and Protection and Electronic Documents Act ("PIPEDA"), and in 2003, Japan enacted the Personal Information Protection Act. These pieces of legislation are just two of many privacy measures that have been taken on the international front. Due to the scale of these countries' economies, the amount of business done with the United States, and the proximity of Canada to the United States, PIPEDA and The Personal Information Protection Act are of particular interest to the U.S. privacy community. Each Act will be individually examined in this piece. The analysis of PIPEDA will focus on the year 2004, while the analysis of Japan's Personal Information Protection Act will begin with its legislative history in 2003, as much of the Act's provisions did not go into effect until April 1, 2005.

II. 2004: PIPEDA AND EMPLOYER VIDEO SURVEILLANCE CAMERAS

On January 1, 2004, the last phase of Canada's federal privacy legislation, the Personal Information and Protection and Electronic Documents Act ("PIPEDA") went into full effect. PIPEDA requires every organization in the course of commercial activity to ensure the protection of individual privacy.[1] After three phases of the Act's implementation, PIPEDA is now fully extended to cover all private and public organizations that collect, use, or disclose personal information. It also covers information about an employee of the organization that the organization collects, uses, or discloses in connection with the operation of federal work, undertaking, or business.[2] As a result, organizations, agencies delegated to ensure PIPEDA compliance, and the federal courts have had to address issues arising from PIPEDA's full extension. In 2004, one of the main issues involved employers' use of video surveillance of their employees in the labor and employment context.

---

[1] Personal Information and Protection and Electronic Documents Act, R.S.C., ch. 5, § 4(1) (2000) (Can.) [hereinafter PIPEDA].

[2] Ann Cavoukian, *The State of Privacy and Data Protection in Canada, the European Union, Japan and Australia*, 748 PRAC. L. INST. 363, 373 (2003).

A. BACKGROUND

1. SCOPE OF PIPEDA

Canada's Parliament enacted PIPEDA on April 13, 2000 "to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions."[3] Based on ten interrelated principles of the Model Code for the Protection of Personal Information, Parliament formed the basis of PIPEDA's core provisions.[4] These provisions require: (1) "every organization" (2) that "collects, uses or discloses" (3) personal information (4) "in the course of commercial activities" to take steps to protect individual privacy.[5] These four elements provide the scope of the Act's applicability.

First, the Act defines an "organization" as an association, partnership, person, or trade union.[6] According to the Office of the Privacy Commissioner, an organization includes both "brick-and-mortar" and e-commerce businesses.[7]

Second, an organization is subject to the Act's provisions in the collection, use, or disclosure of personal information. "Use" is defined as the "treatment and handling of personal information within an organization," whereas "disclosure" pertains to the transfer of data

---

[3] PIPEDA, *supra* note 1, at ch. 5, § 30.

[4] Erika King & John H. Fuson, *An Overview of Canadian Privacy Law for Pharmaceutical and Device Manufacturers Operating in Canada*, 57 FOOD & DRUG L.J. 205, 206-08 (2002) (the ten principles are (1) accountability; (2) identified purposes; (3) consent; (4) limited collection; (5) limited use, disclosure, and retention; (6) accuracy; (7) security; (8) openness; (9) right of access; and (10) compliance).

[5] PIPEDA, *supra* note 1, at ch. 5, § 4(1).

[6] *Id.* § 2(1).

[7] Office of the Privacy Commissioner of Canada, *Backgrounder: The Personal Protection and Electronic Documents Act*, *available at* http://privcom.gc.ca/information/02_06_07_e.asp (last visited Apr. 2, 2005).

outside the organization.[8] The Privacy Commissioner asserts that collection, use, and disclosure are distinct events.[9]

Third, these organizations are subject to the Act's definition of "personal information." "Personal information" is defined as any "information about an identifiable individual."[10] It includes factual information such as an individual's name, age, weight, height, medical records, income, race, ethnic origin and color, marital status, religion, education, and home address and phone number.[11]

Last, the Act applies to "commercial activity," which is defined as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character."[12] The Office of the Privacy Commissioner, however, has not provided much guidance as to this phrase's meaning.[13]

2. THE FINAL PHASE OF PIPEDA

Rather than requiring immediate compliance, Parliament gradually phased in PIPEDA in three stages.[14] In 2001, PIPEDA covered only personal information processed by federally regulated entities, which includes Internet service providers, banks, airlines, and telecommunication companies.[15] In 2002, the Act was extended to cover personal health information, such as information concerning the physical or mental health of the individual, donations by the individual of any body part or any bodily substance of the individual, and

---

[8] Office of the Privacy Commissioner of Canada, YOUR PRIVACY RESPONSIBILITIES: A GUIDE FOR BUSINESSES AND ORGANIZATIONS 2 (2001) [hereinafter GUIDE FOR BUSINESSES].

[9] George Radwanski, Privacy of Commissioner of Canada, Address to the Institute of Canadian Advertising (Feb. 27, 2001), *available at* http://www.privcom.gc.ca/speech/02_05_a_010227_e.asp (last visited Apr. 2, 2005).

[10] PIPEDA, *supra* note 1, ch. 5, § 2(1).

[11] Office of the Privacy Commissioner of Canada, *Your Privacy Rights: A Guide for Individuals to the Personal Information Protection and Electronic Documents Act*, *available at* http://www.privcom.gc.ca/information/02_05_d_08_e.asp (last visited Apr. 2, 2005).

[12] PIPEDA, *supra* note 1, ch. 5, § 2(1).

[13] King & Fuson, *supra* note 4, at 213.

[14] Michael E. Arruda, *PLI Emerging Issues in Online Privacy 2002*, 735 PRAC. L. INST. 57, 70 (2003).

[15] PIPEDA, *supra* note 1, at ch. 5, § 4; *see also* Cavoukian, *supra* note 2, at 373.

information that is collected in the course of providing health services to the individual.[16]

With the last phase now in effect, the Act is no longer limited to federally regulated entities. Instead, PIPEDA is fully extended to cover all private and public organizations that collect, use, or disclose personal information, or information about an employee of the organization that the organization collects, uses, or discloses in connection with the operation of a federal work, undertaking, or business.[17] However, with the Act's full extension into both the private and public sectors, organizations have encountered uncertainties with proper compliance. For example, in 2004, Canada's Office of the Privacy Commissioner, the agency delegated to ensure PIPEDA compliance, has had to address issues involving employers' use of video surveillance of their employees in the labor and employment context.

B. CASE SUMMARY: EASTMOND V. CANADIAN PACIFIC RAILWAY

1. COMPLAINT WITH THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

Erwin Eastmond filed a complaint with the Commissioner's Office against his employer, Canadian Pacific Railway ("CP").[18] Eastmond alleged that CP violated provisions of PIPEDA after CP installed six digital video recording surveillance cameras in the mechanical facility area where he performed his job duties.[19] He argued that the installation of video cameras in the workplace was done in secrecy without any consultation with his union.[20] He asserted further that there was no security problem to justify the video camera installation, that the system could be abused for monitoring conduct and work performance of workers, and that the cameras had a negative effect on employee morale.[21]

---

[16] PIPEDA, *supra* note 1, at ch. 5, § 2.

[17] Cavoukian, *supra* note 2, at 373.

[18] Eastmond v. Canadian Pacific Railway, [2004] F.C. 852, ¶ 2.

[19] *See id.* at ¶ 1.

[20] *Id.* at ¶ 2.

[21] *Id.*

In response to Eastmond's complaint with the Commissioner, CP issued three reasons for installing the cameras. It stated that the cameras were necessary to: (1) reduce vandalism and deter theft; (2) reduce CP's potential liability for property damage; and (3) provide security for staff.[22] To notify its employees, CP posted bulletins in both its diesel and car shops advising all employees and managers of the video camera installations.[23] Also, CP posted signs at all entrance areas around the mechanical facilities that warned individuals that the facility was protected by video and electronic surveillance.[24]

On January 23, 2003, the Privacy Commissioner issued his report.[25] The Commissioner found that Eastmond had a well-founded complaint and recommended that CP remove its video surveillance cameras.[26] The Commissioner's recommendation was based upon his findings of fact applied to subsection 5(3) of PIPEDA.[27] Under that provision, an organization may collect "personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."[28] As a result, the Commissioner believed that he was required to consider: (1) the appropriateness of the organization's purposes for collecting personal information and (2) the circumstances surrounding the determination of those purposes.[29]

The Commissioner concluded that a reasonable person would not consider CP's purposes for collecting personal information appropriate under the circumstances.[30] The Commissioner adopted a four-part test in determining whether CP's use of surveillance cameras was reasonable under the circumstances.[31] Under this test, the

---

[22] *Id.* at ¶ 9.

[23] *Eastmond*, [2004] F.C. at ¶ 5.

[24] *Id.*

[25] *Id.* at ¶ 6.

[26] *Id.*

[27] *See id.* at ¶ 10.

[28] PIPEDA, *supra* note 1, at ch.5, § 5(3).

[29] *Eastmond*, [2004] F.C. at ¶ 11.

[30] *Id.* at ¶ 15.

[31] *Id.* at ¶ 13.

Commissioner looked at whether: (1) the measure was demonstrably necessary to meet a specific need; (2) the measure was likely to be effective in meeting that need; (3) the loss of privacy was proportional to the benefit gained; and (4) there was a less privacy-invasive way of achieving the same end.[32]

CP's installation of video surveillance cameras was not demonstrably necessary to meet a specific need.[33] The Commissioner stated that there were only a few documented incidents of vandalism and theft, most of which had been to the cameras themselves.[34] Further, CP's actual risk from potential liability for the damage of property to third party contractors was unclear.[35] As a result, the Commissioner concluded that though there may be a potential problem, "CP Rail has not demonstrated the existence of a real and specific one."[36]

Because a demonstrable need for video surveillance cameras was not shown, the Commissioner concluded that CP was hard-pressed to argue that the cameras have been a definite deterrent.[37] The Commissioner stated that "[i]n fact, it could be argued that the signs warning people entering the site may have deterred would-be vandals."[38]

CP's installation of video surveillance cameras in its workplace may have caused an adverse psychological effect of a perceived privacy invasion.[39] In balancing the loss of privacy against the benefit gained, the Commissioner recognized that the cameras may possibly identify an individual during the day despite the system's poor picture resolution, "though it would be difficult to do so."[40]

---

[32] *Id.*

[33] *See id.* at ¶ 14.

[34] *Eastmond*, [2004] F.C. at ¶ 14.

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Eastmond*, [2004] F.C. at ¶ 14.

[40] *Id.*

CP did not evaluate whether there was a less privacy-invasive way of achieving deterrence of vandalism and theft, reducing CP's potential liability for property damage, and providing security for its staff.[41] The Commissioner concluded that it did not appear that CP evaluated the cost and effectiveness of alternative means to achieving the same result, such as "better lighting in the parking lots, which could address the issue of employee security, with no effect on employee privacy."[42]

Thus, based on his four-part test, the Commissioner held that a reasonable person would not consider CP's purposes for collecting personal information appropriate under the circumstances. As a result, the Commissioner concluded that CP violated subsection 5(3) of PIPEDA.[43]

2. THE FEDERAL CIRCUIT COURT PROCEEDING

On February 13, 2003, Eastmond initiated a proceeding to the Federal Circuit Court under subsection 14(1) of PIPEDA.[44] Under that provision, "[a] complainant may, after receiving the Commissioner's report, apply to the Court for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report."[45] In initiating the proceeding in the Federal Court, Eastmond sought the following orders: (1) an order confirming the report of the Privacy Commissioner of Canada that CP cease operating and remove the digital video camera system; (2) an order that any records including any videotape recordings in the possession, control, or custody of CP generated by the surveillance system be destroyed; and (3) an order that CP cease and desist from installing non-operational cameras or camera systems in and around its workplaces in Canada, without the consent of the employees' collective bargaining agent.[46]

---

[41] *See id.*

[42] *Id.*

[43] *See id.* at ¶ 15.

[44] *Eastmond*, [2004] F.C. at ¶ 16.

[45] PIPEDA, *supra* note 1, ch.5, § 14(1).

[46] *Eastmond*, [2004] F.C. at ¶ 18.

In evaluating Eastmond's claims, the Court addressed the following issues: (1) whether the Court had jurisdiction to hear Eastmond's complaint; (2) what kind of proceeding was required of the Court under subsection 14 of PIPEDA and how much deference is owed to the Privacy Commissioner's findings; and (3) whether CP breached its PIPEDA obligations.[47]

i. DOES THE COURT HAVE JURISDICTION TO HEAR EASTMOND'S COMPLAINT?

The Court concluded that the dispute between Eastmond and CP fell within the Court's jurisdiction under PIPEDA.[48] Eastmond invoked subsection 14 of PIPEDA as the principle basis under which the Court had jurisdiction over his complaint.[49] CP argued that because the Privacy Commissioner lacked jurisdiction over Eastmond's complaint, the Court also lacked jurisdiction.[50] CP further asserted that because the essential character of Eastmond's complaint involved a dispute arising from the interpretation, application, administration, or violation of the collective bargaining agreement entered into between CP and Eastmond's union, the complaint was under the jurisdiction of an arbitrator.[51]

Under subsection 14 of PIPEDA, two conditions must be met to obtain a hearing by the Court: (1) a complainant must apply to the Court for a hearing; and (2) the hearing must be in connection with any matter in respect of which the complaint is made or that is referred to in the Commissioner's report.[52] The Court concluded that both conditions were met in this instance.[53]

The Court then concluded that the exclusive arbitration model holding under Canada's Supreme Court case, *Weber v. Ontario Hydro*,

---

[47] *See id.* at ¶ 72–88.

[48] *See id.* at ¶ 115.

[49] *See id.* at ¶ 75.

[50] *Id.* at ¶ 72.

[51] *Id.* at ¶ 73.

[52] PIPEDA, *supra* note 1, ch. 5, § 14.

[53] *Eastmond*, [2004] F.C. at ¶ 90.

[1995] 2 S.C.R. 929, was not applicable to Eastmond's complaint.[54] Under *Weber*, the Supreme Court held that if the "essential character of the dispute between the parties arises either explicitly or implicitly from the interpretation, application, administration or violation of a collective agreement, the dispute, if the legislature expressed itself to that effect, is within the sole jurisdiction of an arbitrator."[55] The Court, instead, viewed the issue of standing as between the two statutory regimes of PIPEDA and the Canada Labour Code.[56] Justice Lemieux reviewed other cases in which jurisdictional conflict was at issue and concluded that whether a dispute is within the sole jurisdiction of an arbitrator is dependent upon the essential character of the dispute between the parties.[57] To determine the essential character of a dispute, it was "necessary to look at the nature of the dispute in the factual context in which it arose and the ambit of the collective agreement."[58]

Here, the Court found that Eastmond specifically engaged PIPEDA in his complaint and that there was nothing in the employees' collective bargaining agreement that dealt with personal information and how it may be collected in the workplace.[59] Rather, the agreement only covered disputes over "discrimination, interference, restriction or coercion permitted in the workplace with respect to race, national or ethnic origin, colour [sic], religion, age, sex, marital status, family status, sexual orientation, disability or conviction for which a pardon has been granted."[60] Thus, the dispute between Eastmond and CP did not arise from the collective bargaining agreement, and arbitration was not the proper forum.

---

[54] *Id.* at ¶ 92.

[55] *Id.* at ¶ 108.

[56] *Id.* at ¶ 95.

[57] *See id.* at ¶ 94–109.

[58] *Eastmond*, [2004] F.C. at ¶ 109.

[59] *See id.* at ¶ 114.

[60] *Id.*

ii. WHAT KIND OF PROCEEDING IS REQUIRED OF THE COURT UNDER SUBSECTION 14 OF PIPEDA?

A proceeding under subsection 14 of PIPEDA is not a review of the Privacy Commissioner's report or his recommendation; rather, it is a *de novo* review by the Court, a view CP espoused.[61] Eastmond asserted that in hearing his complaint, the Court should apply the standard of review of the Privacy Commissioner, reasonableness simpliciter.[62] CP, on the other hand, argued that the proceeding before the Court should be a *de novo* hearing, giving no weight to the Privacy Commissioner's findings.[63]

Agreeing with CP, the Court concluded that under subsection 14 of PIPEDA, it is the burden of the person who made a complaint to the Privacy Commissioner to demonstrate that CP violated its PIPEDA obligations.[64] Although the Court recognized that the Commissioner should be accorded some deference in the area of his expertise, the Court failed to accord deference to the Commissioner's findings of fact.[65] The Court stated that the evidence before it was considerably different from that gathered by the Commissioner.[66]

iii. DID CP BREACH ITS PIPEDA OBLIGATIONS?

The Court concluded that CP did not breach its PIPEDA obligations.[67] In making this determination, the Court stated that there were two issues that needed to be addressed: (1) whether CP's reasons for collecting personal information of its employees through surveillance camera recordings were purposes that a reasonable person would consider appropriate under the circumstances; and (2) if CP's purposes were appropriate, whether CP violated its PIPEDA

---

[61] *See id.* at ¶ 118.

[62] *Id.* at ¶ 72.

[63] *Eastmond*, [2004] F.C. at ¶ 77.

[64] *Id.* at ¶ 118.

[65] *See id.* at ¶ 120–33.

[66] *Id.* at ¶ 123.

[67] *See id.* at ¶ 192.

obligations by not obtaining the consent of its employees and others before collecting the information through its cameras.[68]

a. WERE CP'S PURPOSES REASONABLY APPROPRIATE?

The Court held that a reasonable person would consider CP's purposes for collecting data through its video surveillance cameras appropriate under the circumstances.[69] In doing so, the Court adopted the Privacy Commissioner's four-part test that addressed whether: (1) the measure was demonstrably necessary to meet a specific need; (2) the measure was likely to be effective in meeting that need; (3) the loss of privacy was proportional to the benefit gained; and (4) there was a less privacy-invasive way of achieving the same end.[70] The Court noted that this test was in line with Parliament's intent to have a balancing of interests:[71]

> Parliament clearly provided the appropriateness of purposes or why personal information needs to be collected must be analysed [sic] in a contextual manner looking at the particular circumstances of why, how, when and where collection takes place. Also, the appropriate purposes for collection may be different than the appropriate purposes for use and the appropriate purposes for disclosure of collected information, all of which suggests flexibility and variability in accordance with the circumstances.[72]

The Court then cited to previous arbitration cases involving employers' use of surveillance cameras and concluded that arbitrators distinguish between instances of collecting personal information through surreptitious means and instances where employees and others are informed.[73] From these precedents, the Court reasoned that CP

---

[68] *Eastmond*, [2004] F.C. at ¶ 125.

[69] *Id.* at ¶ 174.

[70] *See id.* at ¶ 127–28.

[71] *Id.* at ¶ 129.

[72] *Id* at ¶ 131.

[73] *Eastmond*, [2004] F.C. at ¶ 133–73.

established a legitimate need to have the cameras installed given the "whole of the evidence" by identifying numerous past incidents, which justified the need for the video surveillance cameras.[74] Moreover, the Court concluded that the cameras were an effective means of meeting CP's needs, the loss of privacy was minimal, and CP had looked at alternatives to achieving the same end.[75] On the whole of the evidence, CP established that there had been no recorded incidents of vandalism or theft since the cameras were installed, and that the use of fencing and security guards would disrupt CP's operations.[76] Thus, the Court held that CP's purposes were reasonably appropriate under the circumstances.

b. WAS CONSENT REQUIRED TO COLLECT THE INFORMATION?

CP was able to collect Eastmond's personal information without his knowledge and consent under subsection 7(1)(b) of PIPEDA.[77] Under that provision,

> an organization may collect personal information without the knowledge or consent of the individual only if... (b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province[.][78]

CP argued that the words "except where inappropriate" in subsection 4.3 of Schedule 1 to PIPEDA are self-standing and enable the Court to make a determination of when it is unnecessary to obtain the knowledge and consent of the individual whose personal information is being collected.[79] The Court disagreed. It stated, "the words of an

---

[74] *Id.* at ¶ 177.

[75] *See id.* at ¶ 180–82.

[76] *Id.*

[77] *See id.* at ¶ 189.

[78] PIPEDA, *supra* note 1, ch.5, § 7(1)(b).

[79] *Eastmond*, [2004] F.C. at ¶ 183.

Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament."[80]

In this instance, the Court concluded that CP fell within subsection 7(1)(b)'s exemption.[81] CP established that the videotaped recordings were never viewed unless there was a triggering event and that there was no CP official looking at the monitor when the cameras were operating.[82] As a result, CP collected personal information only when CP officials viewed the recordings to investigate an incident.[83] Thus, PIPEDA's exemption applied.

C. DISCUSSION

1. JURISDICTION

The Federal Court's holding on standing was based on two concurrent statutory regimes operating in concert. On the one hand, PIPEDA provided relief for individuals who satisfied the statutory requirements of subsection 14.[84] On the other hand, the Canada Labour Code mandated that disputes arising under a collective bargaining agreement are to be resolved through arbitration.[85] The Court rejected the Canadian Supreme Court's *Weber* analysis, which would have required the Court to determine whether the legislature intended a dispute to be governed by a collective bargaining agreement or the statutory regime because the two statutory regimes were not in conflict.[86] In other words, a *Weber* analysis is required only "when it is necessary to decide which of the two competing statutory regimes should govern a dispute."[87] The Court concluded that because

---

[80] *Id.* at ¶ 184 (citing *Re* Rizzo & Rizzo Shoes Ltd., [1998] S.C.R. 27, ¶ 21).

[81] *Id.* at ¶ 187.

[82] *See id.* at ¶ 188.

[83] *Id.*

[84] *Eastmond*, [2004] F.C. at ¶ 90.

[85] *Id.* at ¶ 95.

[86] *See id.* at ¶ 99.

[87] *Id.* at ¶ 96 (citing Regina Police Assn. Inc. v. Regina (City) Board of Police Commissioner, [2000] S.C.R. 360, 373–74).

PIPEDA and the Canada Labour Code were not in conflict, to resolve which regime took precedence required the Court to look at whether the "essential character of the dispute" arose either explicitly or implicitly from the collective agreement.[88] Nothing in the Eastmond agreement dealt with personal information and how it may be collected in the workplace.[89] As a result, the essential character of the dispute, i.e. the collection of personal information, did not arise explicitly or implicitly from the collective agreement, and the Court had jurisdiction over the matter.[90]

2. THE *DE NOVO* STANDARD OF REVIEW

The Court in *Eastmond* stated that under subsection 14 of PIPEDA, a *de novo* standard of review was required.[91] Justice Lemieux concluded that because a complaint initiated under PIPEDA was neither an appeal of the Privacy Commissioner's report, nor an application for judicial review, a *de novo* review was appropriate.[92] The Court was unclear, however, as to how much deference should be given to the Commissioner's report. On the one hand, the Court stated that it would "accord the Privacy Commissioner some deference in the area of his expertise which would include appropriate recognition to the factors he took into account in balancing the privacy interests of the applicant and CP's legitimate interest in protecting its employees and property."[93] On the other, the Court stated that it does "not accord any deference on the Commissioner's findings of fact."[94] This limited deference given to the Privacy Commissioner's report gives little guidance for other Courts to apply in the future.

---

[88] *Id.* at ¶ 108.

[89] *Eastmond*, [2004] F.C. at ¶ 114.

[90] *See id.*

[91] *See id.* at ¶ 119 (citing Englander v. Telus Communications Inc., [2003] F.C. 705).

[92] *Id.*

[93] *Id.* at ¶ 122.

[94] *Eastmond*, [2004] F.C. at ¶ 123.

3. THE FOUR-PART TEST

Both the Privacy Commissioner and the Federal Circuit Court agreed on the test to determine whether the purposes for collecting personal information are those a reasonable person would consider appropriate. Under this test, four factors are considered: (1) the necessity of the purpose to meet a specific need; (2) the effectiveness of the purpose in meeting that need; (3) the proportionality of the loss of privacy to the benefit gained; and (4) whether there is a less privacy-invasive way of achieving the same end.[95] However, the Commissioner and the Court disagreed upon the application of the facts. The Court noted that "[t]he Privacy Commissioner took no position on whether the evidence before him...satisfied the four-part test."[96] Applying the facts to the four-part test, the Court distinguished instances where surveillance cameras were used and were not in contravention of PIPEDA, and instances where such usage violated the Act.[97] The Court stated "arbitrators have drawn a bright line between surreptitious collection of information and collection of information by cameras whose locations are known, where employees and others are told recordings are being made and the use of those recordings."[98] This position is consistent with other cases involving PIPEDA.[99]

In *Eastmond*, the cameras were not surreptitiously hidden; rather there were warning signs of their locations.[100] Given the whole of the evidence, the Court concluded that a reasonable person would consider CP's purposes for collecting personal information appropriate under the circumstances.[101]

---

[95] *Id.* at ¶ 127.

[96] *Id.* at ¶ 85.

[97] *See id.* at ¶ 132.

[98] *Id.*

[99] *See* PIPEDA Case Summary #264 (Feb. 19, 2004), *available at* http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_01_e.asp; PIPEDA Case Summary #268 (Apr. 12, 2004), *available at* http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040412_e.asp; *see also* PIPEDA Case Summary #273 (May 28, 2004), *available at* http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040518_e.asp; PIPEDA Case Summary #279 (July 26, 2004), *available at* http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040726_e.asp.

[100] *Eastmond*, [2004] F.C. at ¶ 176.

[101] *Id.* at ¶ 177.

4. CONSENT

After concluding that CP's purposes for installing the surveillance cameras were appropriate under the circumstances, the Court addressed whether CP was required to have employee consent to collect the information.[102] The Court approached the issue as a matter of statutory interpretation.[103] In interpreting subsection 7(1) of PIPEDA, the Court looked at that provision in its entire context, in accordance with the grammatical and ordinary sense of the words in connection "with the scheme of the Act, the object of the Act, and the intention of Parliament."[104]

Subsection 7(1) of PIPEDA was clear in proscribing only four instances where personal information may be collected without knowledge of consent. These instances are: (1) where the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way; (2) where it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information, and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; (3) where the collection is solely for journalistic, artistic, or literary purposes; or (4) where the information is publicly available and is specified by the regulations.[105] In *Eastmond*, the Court determined that the videotaped recordings were not reviewed unless there was a triggering event.[106] Moreover, to ask for permission to collect the information resulting from an investigation would compromise the availability of the information.[107] Thus, CP fell within the second category in which it was not obliged to obtain consent of its employees in obtaining the personal information.[108]

---

[102] *See id.* at ¶ 125.

[103] *See id.* at ¶ 185.

[104] *Id.* at ¶ 184 (citing *Re Rizzo & Rizzo Shoes Ltd.*, [1998] 1 S.C.R. 27, ¶ 21).

[105] PIPEDA, *supra* note 1, ch. 5, § 7(1).

[106] *Eastmond*, [2004] F.C. at ¶ 188.

[107] *Id.* at ¶ 189.

[108] *See id.* at ¶ 187.

D. CONCLUSION

The Federal Circuit Court has made it clear that an employee may invoke PIPEDA to seek redress from an organization that has collected personal information through video surveillance cameras installed in the workplace. Through its four-part balancing test, organizations may utilize the Court's holding as guidance in implementing collection of personal information measures. In the wake of PIPEDA's full extension into both public and private organizations since January 2004, the effects of the Act have been and will undoubtedly continue to be heard through the Canadian court system.

III. THE PERSONAL INFORMATION PROTECTION ACT: JAPAN'S SIGNIFICANT STEP IN LEGISLATING PROTECTION OF PRIVACY

A. INTRODUCTION

On May 23, 2003, the Japanese Diet (Japan's National Legislature) enacted the Personal Information Protection Act.[109] The Act, although not the first piece of legislation passed by the Diet in an attempt to protect the privacy of Japanese citizens, is Japan's most comprehensive piece of privacy legislation to date.[110] Although the Act was passed in 2003, its implementation and enforcement procedures continue to unfold.[111] Japan and its national ministries currently face the challenge of rulemaking and legislative interpretation in both the public and private sectors, balancing the difficulty of compliance with the ever present backdrop of the legislative purpose: protecting its citizens' personal information.[112] American businesses in Japan will also be subject to the Act's provisions. Although many such businesses have taken action in order to ensure compliance with the Act, American businesses may not fully

---

[109] Cedric Laurant & Privacy International, *Privacy and Human Rights 2003: Japan* (2003), *at* http://www.privacyinternational.org/survey/phr2003/countries/japan.htm.

[110] Dr. Masao Horibe, *Privacy and Personal Information Protection in Japan: Past, Present and Future* (Feb. 13, 2003), *at http://*www.export.gov/apececommerce/privacy/2003workshop/horibe.pdf.

[111] Dr. Alan F. Westin, *Greetings From the Director* (Apr. 12, 2004), *at* www.privacyexchange.org/japan/greetings.html.

[112] *Id.*

grasp the Act's effects until enforcement measures are firmly in place.[113]

All of this unfolds, as Columbia University Professor Alan F. Westin, Program Director of the Japan-U.S. Privacy and Data Protection Program has described, during "a time of deep social change in Japan, when the roles of individuals, non-profit organizations, local government, the educational system, and other key areas of Japanese life are in significant transition."[114] This social change may have a direct bearing on how the Act will be interpreted. The Act essentially prescribes how Japanese institutions should protect Japanese citizens' personal information. If Japan's social climate is truly in flux though, interpretation of the Act may vary amongst ministries, regions, and businesses. Interpretation could even be contrary to original notions and assumptions made by the Japanese legislature.

This piece, however, serves not as a predictor of the Act's implementation, but rather as a guide to Japan's Personal Information Protection Act: its history, the body of the Act itself, and a comparative analysis to other countries' privacy legislation. For experts, this piece may serve as a quick reference tool. For non-experts interested in the privacy arena or the Act's effect on American business, it will provide a substantive overview.

B. HISTORY OF THE ACT AND THE PRIVACY BACKDROP IN JAPAN

In 1999, Dr. Westin, with the assistance of Japanese advisor Mr. Jun Sofue, polled one thousand adults drawn from a representative sample of the Japanese population in an attempt to gauge the populace's general attitude toward issues in privacy.[115] The results showed that a strong majority of the populace was worried about privacy issues and the mismanagement of their personal information.[116] For instance:

---

[113] Center for Social and Legal Research, *Japan Privacy Resource on Consumer, Citizen, and Employee Privacy: Privacy Policies*, *at* http://www.privacyexchange.org/japan/japanindex.html (last updated May 6, 2004).

[114] Dr. Alan F. Westin, *supra* note 111.

[115] Dr. Alan F. Westin & Adams Communication Ltd., Japan Privacy Resource on Consumer, Citizen, and Employee Privacy: Reports/Surveys, *Japan National Consumer Privacy Survey* (Dec. 19, 1999), *at* http://www.privacyexchange.org/japan/westinsurvey_ 1999.pdf.

[116] *Id.*

1) 88.8% had read or heard stories in the media about personal privacy in Japan in 1998;

2) 76.6% were concerned about the potential misuse of personal information;

3) 67% believed that consumers had lost all control over how personal information is collected and used by companies; and

4) 65.7% believed that existing law did not adequately protect privacy concerns.[117]

The percentages, although already indicative of a tendency towards popular dissatisfaction with privacy matters in Japan, would have likely been higher if the same poll were taken in 2002. The Japanese media in the years immediately preceding the passing of the Act reported extensively on privacy violations by both businesses and the government in Japan.[118] Most of the privacy violations committed by businesses and reported by the Japanese media involved identity theft and the disclosure of personal information via the Internet.[119] The reports concerning government violations were similar in nature and highlighted the government's negligent handling of citizens' personal information.[120] These media reports could only contribute to the Japanese populace's dissatisfaction and mistrust in both the public and private sectors, as well as serving to notify Japanese officials that action needed to be taken.

Japan did not have national omnibus privacy legislation prior to the enactment of the Personal Information Protection Act.[121] Prior to enactment, the government emphasized self-regulation, and organiza-

---

[117] *Id.*

[118] Dr. Alan F. Westin & Vivian van Gelder, Japan Privacy Resource on Consumer, Citizen, and Employee Privacy: Home/Feature Items, *Special Issue on Consumer Privacy in Japan and the New National Privacy Law: Implications for U.S. Business, Implications for Japanese Companies,* PRIVACY & AM. BUS.: A Comprehensive Report and Information Service (Nov. 2003), *available at* http://www.privacyexchange.org/japan/japanindex.html., page 8.

[119] *Id.* at 8.

[120] *Id.* at 9.

[121] Dr. Masao Horibe, *supra* note 110.

tions associated with government ministries, such as the Japan Information Processing Development Corporation ("JIPDEC"), assisted in this self-regulation.[122] JIPDEC created the "System for Granting Marks of Confidence for Privacy and Personal Data Protection."[123] This system allowed Japanese businesses that were concerned with consumer perceptions of privacy to become certified with JIPDEC. JIPDEC based this certification on the personal data handling guidelines articulated in the Japan Industrial Standard, Q15001.[124] Such certification would presumably increase consumer confidence in that certified business. Although the government emphasized self-regulation, many local governments passed data protection ordinances.[125] By April 2003, 74% of local governments had passed such ordinances.[126] The status of privacy protection in Japan prior to the Act was comparable to the United States' current system. As it currently stands, the United States does not have a single, comprehensive privacy law.[127]

In response to the privacy concerns in Japan, the government organized an expert committee to draft provisions for an omnibus privacy law on January 27, 2000.[128] The expert committee released an outline of the legislation on October 11, 2000, and the bill itself was approved by the Cabinet in March 2001.[129] The bill then moved on to the Diet, where it faced significant opposition. At the forefront of this opposition was the Japanese media.[130] The bill failed to exclude newsgathering activities from its scope, and the media feared that their

---

[122] Westin & van Gelder, *supra* note 118, at 5.

[123] *Id.*

[124] *Id.*

[125] *Id.* at 6.

[126] *Id.* (2413 out of 3260 local governments had passed data protection ordinances.)

[127] PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 2 (1998).

[128] Westin & van Gelder, *supra* note 118, at 11.

[129] *Id.* at 12.

[130] *Id.* at 13.

ability to report the news, especially news involving off-the-record disclosures about politicians, would be thwarted.[131]

The opposition grew in its activity from general rumblings to intense protests spearheaded by media groups.[132] As a result, the bill eventually failed in the Diet on December 13, 2002.[133] The bill was soon revised, and in the revision, the media was granted immunity from the bill's requirements when handling personal information.[134] Although some opposition still remained, the bill was passed on May 6, 2003.[135] According to Dr. Westin and Vivian van Gelder (Legal Director of the Japan-U.S. Privacy and Data Protection Program), the opposition was quelled due to the U.S. invasion of Iraq in March of 2003.[136] The Japanese government supported the invasion, and the government, including the opposition to the Personal Information Protection Bill, turned its attention to these pressing matters in foreign affairs.[137] As a result of this diversion, the Bill was passed.

---

[131] *Id.*

[132] *Id* at 14.

[133] Westin & van Gelder, *supra* note 118, at 15.

[134] *Id.* at 15-16.

[135] *Id.* at 16.

[136] *Id.*

[137] *Id.*

C. THE PERSONAL INFORMATION PROTECTION ACT[138]

What is relevant from the Personal Information Protection Act depends upon who is reading the Act and for what reason. An American business attempting to conduct business within Japan's borders will likely read and contemplate the entire Act. The following is an explication of the Act's most relevant Articles. Some are basic provisions that all privacy scholars should be acquainted with, while others are business-specific.

Chapter 1. Article 1 sets forth the purpose of the Act. Specifically, the Act has the purpose of "protecting the rights and welfare of individuals." Article 1 also assigns responsibility for implementation to both the public (national government and local public entities) and the private sectors (businesses which handle personal information).[139]

Article 2 provides definitions for the Act. "Personal information," as used in the Act, is defined as "information that relates to living individuals and which can be used to identify specific individuals by name, date of birth, or other description (including that which can be easily compared with other information and thereby used to identify

---

[138] The Act's chapters and subchapters are listed here as a reference source for the explication that follows.

The Personal Information Protection Act:
- Chapter 1: General Provisions (Articles 1-3)
- Chapter 2: Duties of National Government and Local Public Entites, Etc. (Articles 4-6)
- Chapter 3: Measures, Etc. for the protection of Personal Information
  - Subchapter 1: Basic Policy Concerning the Protection of Personal Information (Article 7)
  - Subchapter 2: Measures of the National Government (Articles 8-10)
  - Subchapter 3: Measures of the Local Public Entities (Articles 11-13)
  - Subchapter 4: Cooperation between National Government and Local Public Entities (Article 14)
- Chapter 4: Duties, Etc. of Businesses Handling Personal Information
  - Subchapter 1: Duties of Businesses Handling Personal Information (Articles 15-36)
  - Subchapter 2: Promotion of the Protection of Personal Information by Private Organizations (Articles 37-49)
- Chapter 5: Miscellaneous Provisions (Articles 50-55)
- Chapter 6: Penalty Provisions (Articles 56-59)
- Supplemental Provisions

An English translation of the Personal Information Protection Act can be located online at: The Personal Information Protection Act, JAPAN PRIVACY RESOURCE ON CONSUMER, CITIZEN, AND EMPLOYEE PRIVACY: LAWS/REGULATIONS (2003), *available at* http://www.privacyexchange.org/japan/japanindex.html.

[139] *Id.*

specific individuals)." A "principal" is defined in the Act as the individual who is the subject of the personal information.[140]

Chapter 2. Articles 4, 5, and 6 provide the national government and local public entities with the power to devise and execute measures necessary to secure the appropriate handling of personal information.[141] Specifically, the national government is prescribed with "the duty to comprehensively devise [sic] and execute measures necessary to secure the appropriate handling of [p]ersonal [i]nformation in accordance with the spirit of [the] law."[142] Local public entities are given the same power, but they are to devise and execute measures "according to the characteristics of the regions under the jurisdiction of such local public entities."[143] This Chapter provides local governance with some flexibility in implementing the Act.

Chapter 3. Subchapters 2, 3, and 4 describe the power given to the national government and local public entities, and give details of the supportive relationship between the two entities that is to take place as the Act unfolds. Local entities are to be especially supportive to businesses and residents within their areas of jurisdiction. They also are to mediate in the processing of grievances in order to achieve an appropriate and timely handling of such grievances.[144]

Chapter 4. Chapter 4 primarily outlines the duties of businesses handling personal information. This chapter is the most extensive of all the chapters in the Act.

Subchapter 1, Article 15, states that a business must specify, to the extent possible, the purpose for using personal information. If that purpose changes, the change must not exceed the scope "reasonably recognized as having an appropriate connection with the original [p]urpose of [u]se."[145] What is "reasonable" and "appropriate" will surely be subject to scrutiny and interpretation.[146]

---

[140] *Id.*

[141] *Id.*

[142] *Id.*

[143] JAPAN PRIVACY RESOURCE ON CONSUMER, CITIZEN, AND EMPLOYEE PRIVACY: LAWS/REGULATIONS, *supra* note 138.

[144] *Id.*

[145] *Id.*

[146] *Id.*

Subchapter 1, Article 16 states that if a business is to stray from the original purpose of use, consent must be obtained from the principal. Article 16 also states that a succeeding business (e.g., in a merger or acquisition scenario) must use personal information obtained from the previous business within the scope of that previous business's original purpose. If the succeeding business wants to use that personal information for another purpose, the succeeding business must obtain consent from the principal. There are, however, exceptions articulated in Article 16 for when consent is not required if a business is to use personal information outside of the original stated purpose. For instance, if it is necessary for the protection of human life, safety, or property, consent to use the principal's personal information is not required.[147]

Article 17 explicitly forbids a business from obtaining personal information by fraud or other unfair means.[148]

Article 18 states that a business initially acquiring personal information must notify the principal(s) or publicly announce the purpose for the use of the personal information. If the information is acquired by a business via contract from a principal, then the acquiring business must disclose the purpose of use to the principal in advance. Exceptions to the rules articulated in Article 18 are also provided.[149]

Article 19 states that a business handling personal information must diligently attempt to maintain the accuracy of that personal information.[150]

Article 20 prescribes that a "[b]usiness [h]andling [p]ersonal [i]nformation must adopt measures necessary and appropriate for preventing the unauthorized disclosure."[151] Again, what is "necessary" and "appropriate" will surely be subject to interpretation and scrutiny by the government and businesses.[152]

Articles 20 and 21 assign the same "necessary" and "appropriate" standard to the supervision of employees who handle personal

---

[147] *Id.*

[148] JAPAN PRIVACY RESOURCE ON CONSUMER, CITIZEN, AND EMPLOYEE PRIVACY: LAWS/REGULATIONS, *supra* note 138.

[149] *Id.*

[150] *Id.*

[151] *Id.*

[152] *Id.*

information for a business, as well as to delegatees who have been delegated this information in some form by a business.[153]

Article 23 outlines restrictions on businesses providing information to third parties. Essentially, businesses are not to provide information to third parties without the consent of the principal. There are exceptions to this rule of consent, however, and there are situations where a perceived third party may not actually be a third party. Both of these situational categories are also outlined in Article 23.[154]

Subchapter 1, Article 24 discusses various appeasement measures that a business utilizing personal information must undertake for a principal. Items such as the name or title of the business handling the principal's personal information, as well as that business's purpose of use, must be "easily learned" by the principal.[155]

Article 25 states that if a business handling personal information has been requested by a principal to disclose information identifying that principal, then the business must promptly disclose such information. There are exceptions to this rule as well, outlined in Article 25.[156]

Article 27 asserts that if a principal believes an Article 16 or Article 17 violation has occurred, and the business handling the principal's information finds that there are grounds for this charge, then the business must cease using that principal's personal information without delay.[157]

Article 28 provides that if a business handling personal information notifies a principal that it does not plan to take all or a portion of the measures requested by the principal regarding the principal's personal information, or that it plans to take measures different from the principal's request, then it must use its "best efforts" to provide the principal with an explanation of its reasons for that decision.[158]

---

[153] JAPAN PRIVACY RESOURCE ON CONSUMER, CITIZEN, AND EMPLOYEE PRIVACY: LAWS/REGULATIONS, *supra* note 138.

[154] *Id.*

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] JAPAN PRIVACY RESOURCE ON CONSUMER, CITIZEN, AND EMPLOYEE PRIVACY: LAWS/REGULATIONS, *supra* note 138.

Articles 29-31 are procedure-oriented, describing a business's mandated procedure for dealing with requests for disclosure, processing a grievance, etc.[159]

Articles 32-36 primarily discuss the role of the State Minister. Article 32 designates authority in a State Minister to require a business to submit a report detailing the business's handling of personal information for enforcement purposes.[160] Article 34 describes admonishments and orders that the State Minister may issue against a business if the Minister believes that such an action is necessary for the protection of individual rights or welfare. The Minister will look primarily to Articles 16-18 and 20-27 for violations. Article 35 places limitations on the State Minister's authority, while Article 36 describes the State Minister's position and role.[161]

Articles 37-49 outline the formation and the standards that must be followed by private organizations wishing to become involved in the protection of personal information.[162]

Chapter 5. Article 50 provides for exclusions to the Personal Information Protection Act. Exclusions have been created for: (1) broadcast organizations, newspapers, news agencies, or other reporting organizations (essentially all organizations whose purpose is to report); (2) individuals who are writers by trade; (3) universities or organizations having the purpose of scholarly research or individuals belonging thereto; (4) religious bodies; and (5) political organizations.[163]

Chapter 6. Articles 56-59 outline the penalties for noncompliance with the Act. A person who violates an order made pursuant to a provision of Article 34 (admonishments and orders), paragraphs 2 and 3, shall be subject to imprisonment for not more than six months or a fine of not more than 300,000 yen (roughly $3,000 U.S. dollars). Article 32 (collection of reports), and Article 46 (another collection and reports) violations may result in fines not to exceed 300,000 yen.[164]

---

[159] *Id.*

[160] *Id.*

[161] *Id.*

[162] *Id.*

[163] JAPAN PRIVACY RESOURCE ON CONSUMER, CITIZEN, AND EMPLOYEE PRIVACY: LAWS/REGULATIONS, *supra* note 138.

[164] *Id.*

D. THE NEXT STEPS

The public and private sectors have varying responsibilities now to ensure a successful transition into the Act's oversight. With respect to the public sector, the government is mobilizing to coordinate oversight and enforcement of the Act among appropriate Ministries.[165] The Ministry of Health, Labor, and Welfare will supervise privacy issues dealing with employee information under the Act.[166] It is assumed that the Ministry of Finance will oversee privacy issues dealing with financial institutions under the Act, and the Ministry of Trade, Industry, and Economy will likely be charged with oversight for commercial and industrial companies.[167] The Cabinet, as well as the Ministry of Public Management, Home Affairs, Posts, and Telecommunications, will also likely be named to coordinate oversight of the Act within an appropriate sector.[168] Given the broad scope of the Act, it is likely that the government will be forced to draft national industry-specific regulations. At the local level, local government will likely draft individual sector-based laws.[169]

For the private sector, the Act is not yet in operation as of this writing. The provisions affecting the private sector, according to a draft Cabinet order, will come into force April 1, 2005.[170] This provides businesses with time to re-examine their personal information policies and take measures to comply with the Act.[171] However, businesses, both strictly Japanese-based as well as U.S.-based businesses with branch offices in Japan, have started preparing for the April 1 enforcement date.[172] U.S. companies with Japanese offices

---

[165] Westin & van Gelder, *supra* note 118, at 23.

[166] Shinji Kusakabe & Nobuhito Sawasaki, *Data Protection Law Poses Problems for M&A: Japan's New Data Protection Law Limits Access to Personal Information in the Due Diligence Process,* 24 INT'L FIN. L. REV. 1, 4 (2005).

[167] *Id.* at 4.

[168] Westin & van Gelder, *supra* note 118, at 21.

[169] *Id.* at 23.

[170] *Id.* at 22.

[171] *Id.* at 32.

[172] *Japan Privacy Resource on Consumer, Citizen, and Employee Privacy: Privacy Policies, at* http://www.privacyexchange.org/japan/japanpolicies.html. (last updated May 6, 2004).

such as PriceWaterhouseCoopers, Morgan Stanley, Walt Disney, Yahoo!, Apple, McDonald's, Pepsi, Pfizer, and IBM have all created privacy policies that they publicly post on their Japanese-based websites.[173] U.S.-friendly Japanese-based companies are following suit. Companies such as Asahi, Canon, Sony, and Toyota now post privacy policies on their websites as well.[174]

E. U.S. BUSINESS SPECIFICALLY

The Japanese government has written the Act so that only personal information managed in Japan falls within the Act's jurisdiction.[175] Therefore, American businesses with a branch office in Japan must abide by Japan's new privacy legislation when managing information in Japan.[176] At the same time, an American business hoping to do business with Japan, but without any kind of Japanese branch office, will not be under the Act's authority until it actually starts to manage personal information within Japan.

American companies have been fortunate to remain absent from media stories in Japan regarding negligent data handling and sales of personal data.[177] Thus, the ire of the Japanese people has been fixated on Japanese entities, both businesses and the government. There are ambiguities in the Act, though, that in the near future will likely draw attention to American businesses with branch offices in Japan. The new Act appears to lack any restriction on the transfer of personal information originating in but traveling outside of Japan.[178] So, American branch offices can transfer Japanese personal information to their headquarters in America unscathed, assuming that there are no provisions of the Act being violated during that action.[179] More specifically, the Act makes no distinction between transfers of personal information to third parties inside Japan and to third parties

---

[173] *Id.*

[174] *Id.*

[175] Kusakabe & Sawasaki, *supra* note 166, at 2.

[176] *Id.*

[177] Westin & van Gelder, *supra* note 118, at 29.

[178] *Id.*

[179] *Id.*

outside of Japan.[180] This provides American businesses with a great deal of leeway with Japanese personal information, especially because it is not entirely clear that the term "third party" includes subsidiaries, parent companies, or affiliates of a subject business.[181]

According to Dr. Westin and Ms. van Gelder, the major impact of the Act on American companies operating within Japan is the basic preparation that must occur for compliance.[182] Information systems must be upgraded to comply with the new legal requirements for security. A system will also be required to respond to requests in relation to the use of personal data from customers and employees.[183] Also, the Act will have implications on American direct marketing techniques in the Japanese market.[184] Current American marketing techniques rely on the free availability of personal information.[185] American marketers use detailed personal information to match the marketing of products to the consumer, and the Personal Information Protection Act will make it difficult to apply such methods to the Japanese market.[186]

F. A COMPARISON: U.S. – EUROPEAN UNION - JAPAN

In comparing three of the world's most prolific economies, all three have very divergent forms of privacy regulation and legislation. The American system of regulating privacy does not have a single comprehensive privacy law or a single agency charged with administering privacy.[187] Whereas the United States may be considered generally lax with its privacy regulation and legislation, the European Union could be considered to be its polar opposite. The European Union's Directive on Data Protection ("European Privacy Directive"), passed on October 25, 1998, strictly regulates privacy

---

[180] *Id.* at 24.

[181] *Id.*

[182] Westin & van Gelder, *supra* note 118, at 29.

[183] *Id.*

[184] *Id.*

[185] *Id.*

[186] *Id.*

[187] SWIRE & LITAN, *supra* note 130, at 2.

matters within the European Union and also regulates those countries outside of the Union by requiring "adequate" protection from any country that seeks to obtain the personal information of EU citizens.[188]

The European Privacy Directive has, and could continue to have, significant effects on businesses and organizations outside of Europe.[189] In comparison, foreign entities are not obliged to follow Japan's Personal Information Protection Act unless personal information is handled or managed within Japan's borders.[190] The Personal Information Protection Act, then, should not have the same impact on foreign entities as seen by the passing of the European Privacy Directive. There is no foreseeable "collision course" between Japan and other countries, as there was between the European Union and the United States upon the passing of the European Privacy Directive.[191] At the same time, the Personal Information Protection Act is similar to the European Privacy Directive, and quite divergent from U.S. privacy regulation, in that the Act is an omnibus piece of privacy legislation. The Act, however, has a U.S.-type regulation mechanism in that enforcement is sectoral, being charged to various ministries and local government entities.[192] Although the Act is too new to tell whether its "middle way" methodology, somewhere between the poles of the United States and the European Union, will be truly effective, a comparison of these three methods of regulating and legislating privacy may reveal which method should serve as the model for the rest of the international privacy community.[193]

IV. CONCLUSION

In light of privacy legislation on the international front, the dynamic interrelationships between countries require businesses and institutions to cope with these recent privacy developments. The enactment of Japan's Personal Information Protection Act and Canada's PIPEDA illustrate the stark differences to which countries

---

[188] *Id.*

[189] *Id.*

[190] Kusakabe & Sawasaki, *supra* note 166, at 2.

[191] SWIRE & LITAN, *supra* note 130, at 2.

[192] Westin & van Gelder, *supra* note 118, at 32.

[193] *Id.* at 31.

approach privacy issues. As a result, businesses and institutions that conduct international business are forced to comprehend a multitude of legislative provisions that may be in compliance with one country, yet not another. With these uncertainties, businesses have restructured and will continue to restructure organizationally and procedurally in accordance with a country's respective privacy laws to ensure compliance.