UNIFORM STANDARDS TO

PROTECT THE PRIVACY OF PERSONAL INFORMATION

A STUDY OF THE
INTERNATIONAL TREND TO PROTECT
PRIVACY IN PERSONAL INFORMATION

OFFICE OF INFORMATION PRACTICES
MOYA T. D. GRAY, ESQ. DIRECTOR
JEFFREY HESTER, ESQ.
JOHN E. COLE, ESQ.
JANUARY, 2000

THE HISTORY OF DATA PROTECTION LEGISLATION

In the last thirty years the concept of informational privacy protection has developed along with the development of computerized technology. Germany was the birthplace of data protection legislation when the state of Hesse passed the first data protection act in the world in 1970.[1]

Shortly thereafter, in 1978 the State of Hawai`i amended its constitution to specifically include a right to informational privacy that applied to the private sector. It was intended that individuals have the right to control information about them in an increasingly computerized world.

In 1980 the Organization for Economic Cooperation and Development (OECD) issued Guidelines[2] seeking to ensure the free flow of economically necessary personal information by proposing standards that would harmonize different national data protection and privacy legislation schemes.[3] At its 1998 conference in Ottawa, Canada, the OECD Ministers renewed it commitment to these guidelines.[4]

In early 1981 the Council of Europe passed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (European Convention).[5] The European Convention, compared to the OECD Guidelines, placed greater emphasis on human rights and fundamental freedoms rather than on economic development. The European Convention requires that Member Countries enact domestic legislation to protect personal privacy in sensitive information such as health records, race origin, and political and religious beliefs.

---

[1] *See* FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES xiv (1989) [hereinafter FLAHERTY]. FLAHERTY, at 22. Flaherty suggests that "data protection" consists of the privacy interests of individuals in information about themselves which he terms as being the "ultimate values that should serve as the premise for the detailed information-control principles and practices included in data protection."

[2] OECD RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, Sept. 23, 1980 [hereinafter OECD GUIDELINES]. The Guidelines define "personal data" as any information relating to an identified or identifiable individual (data subject), and establish eight basic principles relating to personal data: 1) Collection limitation 2) Data quality; 3) Purpose specification; 4) Use limitation; 5) Security Safeguards; 6) Openness; 7) Individual participation; and 8) Accountability. Id. at 10-11.

[3] *Id.* at 5.

[4] Ministerial Declaration on the Protection of Privacy on Global Networks, OECD Conference A Borderless World: Realising the Potential of Global Electronic Commerce, Ottawa, 7-9 October 1998.

[5] Europ. T.S. No. 108, CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, Jan. 1981 [hereinafter EUROPEAN CONVENTION]. Like the OECD GUIDELINES, the European Convention describes how information is to be treated. *Id.* Art.5-9.

In 1990, the European Union presented an initial draft Directive that would make the protection of personal information uniform throughout the European Union, thereby contributing to the free flow of information within the European Community.[6] A final Directive was adopted as the "Common Position" by the Council of Ministers in 1995.[7] As of September 1999, Belgium, Greece, Italy, Austria, Portugal, Sweden, Finland, and the United Kingdom have implemented the directive. Implementing laws are under consideration by the Parliaments of all other Member States except Germany, France and Luxembourg. These member states are in the process of drafting bills. In those Member States where implementing legislation is not yet in place, individuals are entitled to invoke the Directive's provisions before national courts.[8] While the Directive encourages the free flow of information between Member States by protecting rights of privacy[9] it also requires member states of the European Union to halt the flow of personal information to non-member nations that have inadequate protection of personal information.[10]

Facing a potential embargo of relevant commercial information, countries in the Asia-Pacific region began to legislate privacy protection schemes that would meet the European "adequacy" test without burdening the commercial need for information.

In 1993 New Zealand adopted the New Zealand Privacy Act applicable to both public and private sectors. It contains twelve Information Privacy Principles based generally on the OECD guidelines. In 1994, The Province of Quebec, Canada, enacted its privacy legislation. In 1995 Hong Kong, Special Administrative Region of China adopted its privacy law. The Personal Data (Privacy) Ordinance took effect in 1996, and applies to both the private and public sectors. The processing of personal data must conform to six principles that are based on the OECD principles and cover collection, accuracy, use and security access and transparency. In 1997, the Ministry of International Trade and Industry (MITI) in Japan issued Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector.

In 1999 Canada's federal government introduced privacy legislation and the bill remains alive in the current session. It is also based upon OECD principles. Australia and the State of Victoria have both announced plans to introduce privacy legislation based upon the OECD principles. The nations of Solomon Islands, the Federated States

---

[6] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 24 OCTOBER 1995 ON THE PROTECTION INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (1995) [hereinafter EU DIRECTIVE]. 1995 O.J.(L 281) 23/11/1995 p.003.

[7] *See generally*, Spiro Simitis, *From the Market to the Polis: The EU Directive on the Protection Of Personal Data*, 80 IOWA L. REV. 445 (1995).

[8] Media, Information Society and Data Protection, *Status of Implementation of Directive 95/46* , (last modified Sept. 16, 1999), <http://www.europa.eu.int/comm/dg15/en/media/dataprot/law/impl.htm>.

[9] EU DIRECTIVE, *supra* note 6, at para. 2.

[10] *Id.* at Art. 25.

of Micronesia, Thailand, and possibly Malaysia and Singapore, are currently considering the adoption of privacy legislation.

There is strong interest throughout the United States in the protection of privacy. However, none of the federal agencies have taken a leadership role in this arena. Moreover, privacy legislation that has been adopted tends to obscure, not clarify, the needs of both individuals and businesses for information protection. Professors Paul Schwartz and Joel Reidenberg, in their book[11] conclude that

> limited legal protection does exist and should be recognized…. [The protections]…emerge from direct laws such as Electronic Communications Privacy Act …and from more obscure rules with an indirect effect on the treatment of personal information such as the Federal Financial Institutions Examinations Council regulations…and the employment defamation cases in state courts.…
>
> The existing legal protections tend to focus on access and correction.[12]

The Schwartz and Reidenberg note that the congressional debates in the United States continue to focus on narrow sectorial regulatory philosophy[13]

UNIFORM STANDARDS OF PRIVACY PROTECTION

Despite the worldwide adoption of privacy protection, the debate in the United States has been polarized between American business interests and privacy advocates. American business has fought against any government-imposed regulation on its use of personal information, lobbying instead for self-regulation. On the other hand, privacy advocates point out that self-regulation doesn't work and gives no remedies to individuals for violations Significantly, however, there appears to be little public debate about the initial issues - the adoption of uniform standards of privacy protection. While there are some protections available, there are no uniform standards.

Schwarz and Reidenberg were asked by the European Commission to determine to what extent data processing operations in the United States were guided by privacy principles such as those acknowledged by the European Directive[14] Their findings were

---

[11] *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 153 (1996) [hereinafter DATA PRIVACY LAW]. This book was the result of a study conducted by the authors at the behest of the European Commission to determine the relative position of the United States to that of Europe.

[12] *Id.* §14-1(a), at 382.

[13] *Id.* at 385.

[14] *Id.* §2-2, at 12.

published in the seminal work *Data Privacy Law* in 1996. To compare the United States with the European nations, the authors reviewed privacy legislation across Europe.

Schwartz and Reidenberg found there were four elements that were representative of the standards employed in Europe to protect an individual's privacy interest in personal data. In the most general terms a model approach to implementing legislation protecting the privacy interest of an individual would include the following:

- the establishment of obligations and responsibilities[15];
- the open or transparent processing of personal information[16];
- the creation of a special category of "sensitive" data afforded the highest protection[17]; and finally
- the establishment of an enforceable remedy with oversight by an independent agency.[18]

Each of these points are discussed below.

OBLIGATIONS AND RESPONSIBILITIES

Establishment of a series of obligations and responsibilities for the treatment of personal information creates the framework for fair treatment of personal information whether by the government or by business.[19] Once the framework in created, predictability is inserted in the electronic and geographic marketplace and both consumers and businesses will benefit.[20] These obligations and responsibilities include that

- personal data be collected and processed only for specific purposes[21]
- use of the personal data is limited to only those uses that are compatible with the stated purpose of collection[22]

---

[15] *Id.* §2-2(a), at 13.

[16] *Id.* §2-2(b), at 15.

[17] *Id.* §2-2(c), at 16.

[18] *Id.* §2-2(d), at 16.

[19] *Id.* §2-2(a), at 13.

[20] Joel R. Reidenberg & Françoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, WAKE FOREST L. REV. 105, 108-9 (1995) (authors noting that while individuals certainly have an interest in the treatment of personal information, businesses also benefit by having a structure in place to ensure the quality and integrity of the information upon which they must rely). *Id.*

[21] OECD GUIDELINES, *supra* note 2, Purpose specification principle ; EUROPEAN CONVENTION, *supra* note 5, Art. 5(b); EU DIRECTIVE, *supra* note 6, Art. 6(b).

- the collected information is relevant to those purposes and places limits on the collection of extraneous or unnecessary information[23]
- duration of storage of personal data be limited[24] and
- the integrity of the data is ensured by requiring appropriate security measures.[25]

The Hawai`i 's Fair Information Practices Act, which was repealed when the legislature adopted the Uniform Information Practices Act (Modified) ("UIPA") in 1989, included subject access and correction rights and limitations on disclosure.

While the State of Hawai`i,[26] the federal government and some private sector industries do give individuals the right of access and correction, larger parts of the private sector in the United States have not yet embraced this principle of subject access.

Personal information is typically considered propriety information of the businesses that hold it -- not the property of the individuals to whom it pertains. The characterization of this information as proprietary to the business is the result of the key competitive advantages to those companies with the most thorough customer profiles.[27] For example, the authors of this study were advised of a lawsuit in which a securities salesman changed employers and took with him a list of customers and their personal information. The former employer sued the salesman for the customer list, alleging it was proprietary information.[28]

There does not appear to have been concern about the desires of the people from whom the information was collected. Does American business perceive its interest in this information as deserving more protection than the individuals from whom the information was collected? Giving individuals access to this information is perceived as violating the sanctity of proprietary information.[29] Nevertheless, access to personal

---

[22] OECD GUIDELINES, *supra* note 2, Use Limitation principle; EUROPEAN CONVENTION, *supra* note 5, Art. 5(b); EU DIRECTIVE, *supra* note 6, Art. 6(b).

[23] OECD GUIDELINES, *supra* note 2, Data Quality principle; EUROPEAN CONVENTION, *supra* note 5, Art. 5(c); EU DIRECTIVE, *supra* note 6, Art. 6(c).

[24] OECD GUIDELINES, *supra* note 2, Data Quality principle; EUROPEAN CONVENTION, *supra* note 5, Art. 5(e); EU DIRECTIVE, *supra* note 6, Art. 6(e).

[25] OECD GUIDELINES, *supra* note 2, Security Safeguards principle; EUROPEAN CONVENTION, *supra* note 5, Art. 7; EU DIRECTIVE, *supra* note 6, Art. 6(e).

[26] *See* §§92F-23 to -25, Hawaii Revised Statutes.

[27] Reidenberg & Gamet-Pol, *supra* note 20 at 120.

[28] Conversation with Securities Commissioner for the State of Hawaii, the Honorable Ryan S. Ushijima, Dec. 12, 1999.

[29] DATA PRIVACY LAW §12-1(a)(5) , *supra* note 11, at 325-27.

information is an enforcement mechanism that is critical to effective protection of personal information[30]

TRANSPARENCY IN DATA PROCESSING

The second element necessary to the protection of personal information is the transparent processing of this information.[31] Transparent or open processing of personal information is the mechanism by which an individual has control over his or her personal information. Open processing gives the individual the ability to find out who is collecting the information, what information is being processed and how the data is being treated.[32] As Schwartz and Reidenberg said

> [I]ndividuals must be able to comprehend the treatment of their personal information to participate in social and political life. Secretive processing of personal information risks the suppression of an individual's free choice.[33]

Obviously, to be transparent, individuals must be told that information is being collected about them. As databases of personal information are sources of power and profit for large institutions and the government, the "transparency" element explains the importance of keeping their information practices subject to public scrutiny.[34] Notification keeps the entire process open and encourages the data subject's participation in monitoring his or her own information.[35]

Business in the United States may take the position that it is too costly and a burden to notify each customer that it collects information from. But this argument is deceptive because some industries that use personal information are already required to provide notice and others give minimal notices on web sites.

In the range of choices available, notification can be either to the individual directly or to a monitoring agency.[36] Where data protection legislation does not require

---

[30] *See* Reidenberg & Gamet-Pol, *supra* note 20, at 110. *See also EC Privacy Directive and the Future of U.S. Business in Europe: A Panel Discussion*, 80 IOWA L. REV. 669, 675, Citibank thinks there is a need for a data protection authority in the U.S., *Id.*

[31] DATA PRIVACY LAW § 2-2(b) , *supra* note 11 at 15.

[32] OECD GUIDELINES, *supra* note 2, Openness principle; EUROPEAN CONVENTION, *supra* note 5, Art. 8; EU DIRECTIVE, *supra* note 6, Arts. 10-11.

[33] DATA PRIVACY LAW §2-2(b) , *supra* note 11, at 15.

[34] FLAHERTY, *supra* note 1, at 9.

[35] Reidenberg & Gamet-Pol, *supra* note 20, at 109.

[36] *See* Robert G. Schwartz, Jr., *Privacy in German Employment Law*, 15 HASTINGS INT'L & COMP. L. REV. 135, 141 (1992); Privacy Act, 1993 (N.Z.), Art. 6 (3) [hereinafter New Zealand Privacy Act]; *See*

individual notification, the individual can discover whether information concerning him is being collected,[37] but through a registration list filed with the monitoring agency.[38] This method requires that the business collecting personal information state its purpose for the collection of personal information and disclose any intended recipients of this information.[39]

HEIGHTENED PROTECTION FOR SENSITIVE INFORMATION

The third element involves creating a higher level of protection for "sensitive" information.[40] "Sensitive" information is that which relates to racial origin, political opinions or religious beliefs, criminal convictions, information relating to one's sexual life and one's health information.[41] It is apparent that unauthorized disclosure or unintended uses of this type of intimate personal information could have drastic repercussions.[42] The volatile nature of this category of information helps to explain why it has received the majority of the United States' limited attention to this area.[43] The overall lack of protective legislation coupled with the advance of data processing capabilities has caused the trading of "sensitive" information to become ominously commonplace.

---

also, Data Protection Act, 1984, ch. 35, Art. 21(1)(b) (Eng.) [hereinafter British Data Protection Act]; Quebec Access to Information Act §89 (1982)(Can.).

[37] British Data Protection Act, *supra* note 36, Art. 21(1)(b); Quebec Access to Information Act, *supra* note 36, §89.

[38] For example, the British Data Protection Act requires the Data Protection Registrar (monitoring Agency) to keep open for public inspection a register of companies or agencies that hold personal information. British Data Protection Act, *supra* note 36, Arts. 4-9.

[39] There is generally also a requirement that any response to an individual's request for his or her personal information be in a form readily understandable or able to be deciphered. This safeguard prevents businesses or agencies from disclosing requested personal information in a highly technical format and aids in keeping their personal information practices subject to public scrutiny.

[40] DATA PRIVACY LAW §2-2(c) , *supra* note 11, at 16.

[41] EUROPEAN CONVENTION, *supra* note 5, Art. 6; EU DIRECTIVE, *supra* note 6, Art. 8.

[42] *See* Jay Greene, *They're Selling Your Secrets*, ORANGE COUNTY REGISTER, April 21, 1996 at A01. (An employer looking to cut costs examined employee prescriptions and discovered an employee with high prescription bills to be taking medication for AIDS, the employee sued for emotional distress but ultimately lost).

[43] *See* the Video Privacy Protection Act of 1988, 18 U.S.C. 2710, prohibiting the release of video rental records. (It is known as the "Bork Bill" because it was passed during Robert Bork's Supreme Court nomination after Congress discovered Mr. Bork's video rental records had been examined by investigators, *See* INFORMATION POLICY COMM., NAT'L INFORMATION INFRASTRUCTURE TASK FORCE, OPTIONS FOR PROMOTING PRIVACY ON THE NATIONAL INFORMATION INFRASTRUCTURE 42 (1997) [hereinafter OPTIONS PAPER].

This special category of information is specifically addressed in Europe and elsewhere, where an individual's privacy is recognized as a fundamental right susceptible to infringement.[44] This conception stems in part from the differing legal tradition but more importantly reflects recognition of the dangerous impact that a technologically dynamic society operating in a static legal process can have on individual privacy.[45] Therefore, a data protection regime should acknowledge requires the element that "sensitive" information receive the highest protection afforded by law.

ENFORCEABLE RIGHTS AND INDEPENDENT OVERSIGHT

The final element is the establishment of enforceable rights and independent oversight of information practices.[46] This element provides a mechanism that both addresses real harms and weeds out negligible complaints. Individuals who have been harmed by disclosure of their personal data are given an enforceable remedy and a forum to enforce this remedy. Businesses have a regulator that knows the industry and has built up a solid knowledge base concerning that industry. An independent[47] agency, where redress can be had without resorting to the judicial system, enhances the effectiveness of all the other elements in this model approach.[48]

An oversight authority should be tasked with ensuring the free flow of information in a manner that protects the privacy of personal information. Indeed, the best approach would find the agency in a balance between enforcing the rights of the people and promoting a more structured transfer of personal information.[49] For example, outside of Europe, the preferred approach is a framework where individuals are given an enforceable right, but private sector businesses relying heavily on the flow of information are not extraordinarily burdened.[50]

---

[44] *See* FLAHERTY, *supra* note 1, at 34 (discussing the German conception of data protection encompasses an individual's personality or a personal sphere which needs special protection).

[45] *See* Simitis, *supra* note 7, at 447-449.

[46] DATA PRIVACY LAW §2-2(d), *supra* note 11, at 16.

[47] *See* FLAHERTY, *supra* note 1, at 166. (The highly politicized nature of government in France limits the effectiveness of the CNIL as an independent body because it has been unwilling to confront government practices).*Id.*; *See also* Spiro Simitis *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 744 (1987).

[48] *See* OFFICE OF THE DATA PROTECTION REGISTRAR, THE GUIDELINES, ch.5, §7.1 at 84; Paul-Andre Comeau & Andre Ouimet*, Freedom of Information and Privacy: Quebec's Innovative Role in North America,* 80 IOWA L. REV. 651, 666 (1995).

[49] *See* Reidenberg & Gamet-Pol, *supra* note 20, at 123-125 (1995). (discussing the shifting attitude of business towards the acceptance of legal rules).

[50] In Quebec for example there is no registration for businesses with databases of personal information, Comeau & Ouimet, *supra* note 48, at 667.

In cases of self-regulation by industries through the establishment of internal codes of conduct the problem has always been enforcement.[51] For example, self-regulation of personal information on the Internet seems to have failed. Self-regulatory privacy seal programs attempt to include many aspects of fair information handling, but typically are ineffective because they have little power to enforce compliance. These programs are also used by only a small fraction of web sites, leaving the consumer to surf at his own risk through the majority of the Internet.

Further, privacy seal programs on the Internet can lead to a false sense of security--this is illustrated in the unfair trade practices complaint filed with the Federal Trade Commission against TRUSTe and America Online.[52] The complaint alleges that both TRUSTe and AOL claim that the seal program covers the "AOL.COM" web site. However, the seal covers only a small portion of the site, "www.aol.com," but not the members' area.[53] When a person visits www.aol.com they see the TRUSTe seal, but if they decide to join, they are transferred to the members area where personal information is collected and then released to telemarketers.[54] The Internet is an arena where the potential for the misuse of people's personal information is immense.

Although pure self-regulatory efforts are proceeding, they are not sufficient to protect the privacy of personal information. Unlike self-regulation, the cooperation between business and the overseeing authority in the development of these standards or codes of conduct can place accountability for fair information practices on each business and yet be tailored to fit the needs of a particular industry. While the standards may differ slightly from industry to industry, an individual may still seek redress in a single agency, which simplifies the administrative procedure. This makes enforcement a realistic and achievable result.[55]

In conjunction with the development of industry standards, the agency responsible for monitoring the implementation of fair information practices becomes a clearinghouse where all parties can thoroughly and clearly discern their respective rights and obligations.[56] This element of oversight is indispensable because it binds together the other elements into a symbiotic unit of well-defined obligations – this ultimately creates greater reliability in the enforcement mechanism.

---

[51] Reidenberg, *supra* note 4, at 508 (1995).

[52] *Unfair Trade Practices Complaint Filed Against Truste/AOL*, PRIVACY.NET, <http://www.privacy.net/truste.asp>.

[53] *Id.*

[54] *Id.*

[55] In New Zealand, an individual may complain to the Privacy Commissioner for any violation of the Privacy Principles by any person, corporate or otherwise, public sector or private sector. *See* N.Z. Privacy Act, Art. 2, 67.

[56] *See* Simitis, *supra* note 47, at 742-744.

ASIA-PACIFIC MODEL

The Asia-Pacific model was first promulgated in New Zealand in 1993. Just recently, in a review prepared by the Office of the Privacy Commissioner for New Zealand, Mr. Stewart wrote:

> Compliance costs arising from legislation has been an issue for governments for some time. Indeed, the desire to minimise costs was an explicit consideration in the design of the Privacy Act 1993. The 1987 report for the Minister of Justice on the proposed shape of privacy legislation, *Data Privacy: An Options Paper,* steering New Zealand away from the more burdensome licensing and registration models current in Europe for just such reasons.[57]

Since that time there have been other iterations of that model. The model generally meets the four elements discussed previously. However, the model takes a less regulatory approach to privacy than does the European model by involving business in the development of codes of practice.

The Asia-Pacific model sets clear standards, creates an independent oversight authority which has specific authority to adopt specific "codes of practice" which bind specific industries to particular standards that may vary from the standards set in the statute, and gives individuals specific rights of action usually with the independent oversight authority and not with the courts in the first instance. The following is a summary of those countries that have proceeded to adopt the Asia-Pacific model, or a variation.

NEW ZEALAND

The New Zealand Privacy Act, adopted in 1993, contains twelve Information Privacy Principles based generally on the OECD guidelines. Except for the right to access and correction, there was no private right of action for violations for a 3-year period. This ensured the private sector adequate time to adapt their business practices to the standards. The Office of Privacy Commissioner was created to oversee and enforce the Act.

The Principles can be individually or collectively replaced by enforceable codes of practice for particular industry sectors or classes of information. The Commissioner has had occasion to adopt only one complete sectoral code, the Health Information Privacy Code. Other codes of practice that alter the application of single information

[57] Blair Stewart, Manager, Costs and Legislation, Office of the Privacy Commissioner of New Zealand, from his compilation of material relating to compliance and administration costs from the review consultations conducted in mid 1997 as required by the Privacy Act, dated May 1998.

privacy principles include the Superannuation Schemes Unique Identifier Code, the EDS Information Privacy Code, and the Justice Sector Unique Identifier Code.

The act does not establish a statutory tort of invasion of privacy and people cannot sue in the courts.[58] Complaints by individuals are filed with the Commissioner who resolves the matter. Recourse to civil remedies is allowed only after the privacy commissioner has decided to take the investigation no further.

The Act has received the support of New Zealand's private sector. The NZ Employers Federations stated that "[a]lthough any 'non-business' cost is an imposition on business, to date it does not appear that compliance costs are excessive." The Insurance Council of New Zealand stated that

> With regard to the rest of the Privacy Act 1993, our members do not report any major difficulties and have found that compliance is largely a matter of good business practice.

HONG KONG

Hong Kong, Special Administrative Region of China, adopted its privacy law in 1995. The Personal Data (Privacy) Ordinance took effect in 1996, and applies to both the private and public sectors. The processing of personal data must conform to six principles, which are based on the OECD principles and cover collection, accuracy, use and security access and transparency. The Ordinance imposes additional restrictions on data matching, direct marketing, and transborder data transfers. The Commissioner may also issue codes of conduct to provide guidance on compliance with the Ordinance's general provisions.

The Privacy Commissioner is given strong enforcement powers that include the power to initiate investigations and conduct audits of those suspected of contravening the Ordinance. The Commissioner has issued numerous advisory/warning and enforcement notices, and referred numerous cases to the police for prosecution.

Hong Kong's first Privacy Commissioner, Stephen Lau, has recently reported wide acceptance in the community of the privacy law.

AUSTRALIAN PROPOSAL

Like Hawai`i , Australia has statutory privacy protection for records held by the Australian government. The Privacy Commissioner for Australia, Malcolm Crompton,

---

[58] Bruce Slane, PRIVACY PROTECTION: A KEY TO ELECTRONIC COMMERCE, PAPER BY THE PRIVACY COMMISSIONER, BRUCE SLANE, ON THE OCCASION OF THE APEC ELECTRONIC COMMERCE STEERING GROUP MEETING, AUCKLAND, 27, JUNE 1999.

has just announced that the federal government has proposed privacy protection for private sector records. The public parts of the proposal indicate that Australia's current government will also proceed with the Asia-Pacific model.

The State of Victoria, under a liberal government, proposed a Data Protection Bill in 1998 that follows the elements of the Asia-Pacific model. The new labor government intends to introduce a data protection bill into parliament this coming session.

CANADIAN PROPOSAL

Canada[59] also has statutory protection for records held by the Canadian government. Canada's Privacy Commissioner, Bruce Phillips, reports that the government introduced privacy legislation in 1999 and the bill remains alive in the current session. The Canadian model is a mix between the European Model and the Asia-Pacific Model, in that it sets out clear standards, creates privacy commissioner but does not give the commissioner the capacity to adopt codes of practice. The Canadian model gives the commissioner tremendous power to enforce the law, including entering the premises of an organization for purposes of investigations.

The Provinces of British Columbia, Alberta, and Ontario all have Freedom of Information and Privacy offices, which are substantively similar to the Office of Information Practices.

JAPAN

Japan adopted a model that has some similarities to the Asia-Pacific model. It has adopted a "privacy mark" system that is administered by a joint public/private agency the Japan Information Processing Development Center.[60] In 1997, the Ministry of International Trade and Industry (MITI) issued Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector. A Supervisory Authority was created to monitor a system for granting "privacy marks" to businesses committed to following the MITI guidelines, and to promote consumer awareness of privacy protection.[61] Businesses not complying with the guidelines, will not be given the privacy protection mark, and presumably be penalized by market forces. The Supervisory Authority will also investigate violations and make recommendations to the appropriate authorities as warranted.[62]

---

[59] The Province of Quebec was the first jurisdiction in the Americas to adopt comprehensive privacy legislation in 1993.

[60] Electronic Privacy Information Center, PRIVACY AND HUMAN RIGHTS, AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 97 (1999).

[61] *Id.*

[62] *Id.*

CONCLUSION

The Office of Information Practices concludes that the Asia-Pacific model of personal information protection in the private sector is best suited to the State of Hawaii. Its combination of enacting basic privacy standards, allowing for the development of industry specific standards, educating the public concerning their rights, and adjudicating disputes between individuals and private parties is more consistent with the American philosophy of government's role.