THE PRINCIPLE OF SECURITY SAFEGUARDS:

ACCIDENTAL ACTIVITIES

Rasika Dayarathna

Department of Computer and Systems Sciences (DSV), Stockholm
University/Royal Institute of Technology
Forum 100; 164 40 Kista, Stockholm- Sweden.
si-ika@dsv.su.se

ABSTRACT

The principle of information security safeguards is a key information principle contained in every privacy legislation measure, framework, and guideline. This principle requires data controllers to use an adequate level of safeguards before processing personal information. However, privacy literature neither explains what this adequate level is nor how to achieve it. Hence, a knowledge gap has been created between privacy advocates and data controllers. This paper takes a step to bridge the aforementioned knowledge gap by presenting an analysis of how data protection and privacy commissioners have evaluated the level of adequacy of security protection given to personal information in selected privacy invasive cases. This study addresses security measures used to protect personal information against accidental incidents. This analysis also lays a foundation for building a set of guidelines for data controllers on designing, implementing, and operating both technological and organizational measures used to protect personal information.

KEY WORDS

Information privacy, information security, accidental disclosure, accidental loss, personal information.

THE PRINCIPLE OF SECURITY SAFEGUARDS:

ACCIDENTAL ACTIVITIES

1 INTRODUCTION

Privacy principles are the basic building blocks of privacy standards which include privacy directives, legislation measures, guidelines, frameworks and industry best practices. One of the key information privacy principles is information security safeguards. According to the Organisation for Economic Cooperation and Development (OECD), the principle of security safeguards states that "personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data"(OECD, 1980). The EU Directive 95/46/EC mentions this principle in Articles 17 and 25. Article 17 prohibits the processing of personal information without providing an adequate level of protection for personal information and Article 25 prohibits the transferring of personal information to a third country that does not have an adequate level of protection for personal information. Every year a significant number of complaints pertaining to the violation of this principle are received by privacy and data protection commissioners. For example, during the period of 2004-05, the Hong Kong privacy commissioner received 131 complaints; this amounts to 14% of the total cases (HG-Annual Report, 2006). This paper presents the measures suggested by privacy and data protection commissioners for the protection of personal information against accidental incidents.

What does this principle state? Is it synonymous with information security? According to the explanatory notes of the OECD's privacy guidelines (OECD, 1980), privacy and security are two different things. Information security focuses on providing confidentiality, availability, and integrity to informational assets of organizations. In contrast, the principle of security safeguards in information privacy focuses on achieving a "reasonable" or "adequate" level of protection, not "perfect" or "maximum" protection for personal information of natural persons. Natural persons include customers, employees, employers, and other stakeholders.

Personal information often falls into organizational information assets. However, personal information belongs to outsiders who have given their personal information to organizations for specific purposes and time period. Therefore, this author argues that extra care must be taken in respect to personal information. In order to provide better protection, there should be appropriate security standards. According to Iachello (2003), existing multi-national and domestic security standards and best practices have not sufficiently covered information privacy aspects.

Another conflicting aspect is that information security heavily focuses on protecting informational assets from external parties. However, reported cases have shown that a large number of information privacy threats are posted by insiders including organizations themselves (Muelle & Rannenberg, 1999). As a result of focusing heavily on outsider attacks, the current evaluation schemes do not provide adequate attention for multilateral security. In certain cases, it can be seen that information security and privacy lead to conflicting situations. For example, some information security requirements such as keeping backups in many locations or monitoring employees' activities conflict with information privacy requirements. In addition to that, information privacy legislation measures give certain inalienable rights to data subjects such as accessing personal information and making corrections (Opinion 1/98, 1998). Unless data controllers take appropriate measures, exercising these rights threatens information assets. Another conflicting issue is that information security entails and eagerness to acquire more personal information, but legal privacy legislation measures prohibit excessive use of personal information. For instance, the use of fingerprints found on a student's canteen was considered to be privacy invasive by the Swedish data protection commissioner.

1.1 Advantage

There is a dilemma that states technologists can not precisely understand what legal advocates and legislators say (Dempsey & Rubinstein, 2006). One aim of this study is to present legal privacy requirements imposed in the principle of security safeguards in an understandable manner to technologists. It is also expected that this will assist technologists to precisely understand their legal privacy obligations in designing and operating information systems. The main aim of this paper is to understand

the notions of ‘adequate’ or ‘reasonableness’ mentioned in privacy standards. This understanding is necessary for choosing appropriate organizational and technological measures for protecting personal information.

1.2 Methodology

Without defining what ‘adequate’ or ‘reasonable’ means in privacy legislation measures, competent bodies are given a mandate to decide whether a measure is adequate/reasonable or not. This paper followed the Common Law tradition, which analyzes and interprets previously given decisions and judgments by legal authorities in judging a present case. It is expected that analyzing and interpreting verdicts given by data protection and privacy commissioners sheds lights on understanding what an adequate or reasonable level is. There are cases that fall into one or more information privacy principles. The criterion used to identify whether a case relates to this principle is an allegation that an event occurred due to the lack of appropriate organizational and technological measures.

1.3 Materials and Methods

This study covers some national data protection legislation measures, regional directives, privacy guidelines, and frameworks introduced by leading privacy organizations and verdicts given by selected data protection and privacy commissioners. The studied directives, frameworks, and guidelines are Article 17 of EU Data Protection Directive 95/46/EC, Principle 7 of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework (APEC, 2005), Section 16 of the APEC Privacy Charter (Greenleaf & Waters, 2003), Article 7 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CECPI/APPD) ¬Convention No 1981, the AICPA/CICA Privacy Framework (AICPA/CICA, 2004) introduced by the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA), and OCED Privacy Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 1980). The EU Directive and CECPI/APPD cover the whole Europe and APEC Privacy Framework Charter cover some Asia-Pacific countries while the OECD covers a large number of industrialized countries. The

AICPA/CICA Privacy Framework is the base for the 'WebTrust' web privacy seal, which is one of the leading online privacy seals.

First, the principle of information security was analyzed and functional requirements imposed by the principle were identified. In this examination, six privacy directives, legislation measures, and frameworks were used. Second, verdicts given by data protection and privacy commissioners were scrutinized to identify underlying privacy threats. Based on the identified threat, a verdict was placed under one of the identified functional requirements derived in stage 1. Then, the recommended organizational or technological measures were identified and presented accordingly. There are certain cases where the commissioners have not suggested protection measures. In those cases, appropriate measures are suggested to give a rough picture of possible solutions. However, these measures are not comprehensive. In addition, some expected privacy threats are given for cases where there is no involvement of ICT but may be interpreted similarly.

1.4 Analysis

Seven legal privacy threat categories were identified in analyzing the principles: accidental loss and disclosure, unauthorized access, use, destruction, alteration and disclosure. The criterion applied in differentiating accidental and unauthorized activities is discussed in Section 1.5.

Table 1 shows the high-level requirements imposed in the principle. On the horizontal axis, high-level requirements are given under three categories: accidental, unauthorized, and others. The first category, accidental, covers all kinds of accidental privacy breaches which include access, use, destruction, loss, alterations, and disclosures. The second category covers unauthorized access, use, destruction, alterations, and disclosure. The last category covers any other kind of misuse. For example, the EU Directive 95/46/EC states that measures should be taken as a protection from all other unlawful forms of processing. The vertical axis provides the identification of the studied privacy literature (data protection directives, frameworks, charter, and guidelines). When a high-level requirement is explicitly mentioned in a given piece of literature, the corresponding box is marked with 'Y'; otherwise, it is left blank. Cases

where high-level requirements are given in a similar term are presented with superscripts and discussed in the legend.

Table 1: High-level requirements imposed in the principle of security of safeguards according to the studied international privacy literature.

	Accidental						Unauthorized					Other
	Access	Use	Destructio	Loss	Alteration	Disclosure	Access	Use	Destructio	Alteration	Disclosure	
CECPI/APPD			Y	Y			Y	Y	Y	Y	Y	
OECD				Y			Y	Y	Y	Y[3]	Y	
EU DPA			Y	Y	Y		Y		Y[4]	Y	Y	Y[5]
APEC Charter	Y	Y		Y	Y[1]	Y	Y	Y		Y[3]		Y
APEC Privacy				Y			Y	Y	Y	Y[3]	Y	Y
AICPA				Y			Y	Y[2]	Y	Y	Y	

Superscripts stand for: Y1 accidental modification, Y2 misuse, Y3 unauthorized modification, Y4 unlawful destruction and Y5 all other unlawful forms of processing. APEC Charter and APEC Privacy stand for the APEC Privacy Charter and the APEC Privacy Framework respectively.

All studied literature emphasizes the accidental loss component of the principle. Only the European literature mentioned accidental destruction. The EU Directive mentions “alteration” without specifying whether it refers to accidental or unauthorized alteration. The predecessor of the APEC Privacy Framework, APEC Privacy Charter, specifically mentions accidental access, use, and disclosure. Taking the above points into account, the accidental threat category has been divided into accidental loss and destruction and accidental disclosure.

1.4.1 Factors affecting the adequate level of protection

Legal privacy literature presents factors that affect adequate levels of protection. Table 2 presents the factors given in EU Directive 95/46/EC, the Canadian Personal Information Protection and Electronic Documents Act, the old Swedish Data Protection Ordinance, and the PISA (Privacy Incorporated Software Agents) project documentation. The old Swedish Data Protection Ordinance and the PISA documentation have defined privacy risk classification schemes based on these factors.

Table 2: Factors affecting the level of reasonableness as defined in the principle of security safeguards

	EU Directive	Canadian Law	PISA	Swedish Ordinance
Nature of PI	Yes	Yes	Yes	Yes
Cost factor	Yes			
State of the art	Yes			
Processing risk	Yes		Yes	
Amount of PI		Yes	Yes	
Distribution		Yes		
Format		Yes		
Storage method		Yes		

PI stands for personal information. According to Article 8 of the Directive 95/46/EC, sensitive data are racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, and sex life. The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) states the sensitivity of personal data depends on the context. However, it gives medical records and income records as examples for sensitive personal data. According to privacy legislation measures, sensitive personal information should be given additional protection.

Data protection legislation measures insist on taking organizational and technological measures to protect personal information, but they do not mention what those measures are. However, Section 4.7.3 of the PIPEDA sheds lights on those measures. Instead of giving precise definitions, the act

gives some examples. Examples given for physical access are locked filing cabinets and restricted access to offices; organizational measures are security clearances and limiting access on a "need-to-know" basis; technological measure are the use of passwords and encryption. Based on the above, these measures can be explained. Organizational measures cover all administrative measures such as drafting policies, recruiting people, allocating resources, and providing training with special focus on data protection. Physical measures to cover access to office premise and locations where information system and personal information reside. Technological measures include all measures used to protect personal information and system based on data and software.

1.4.2 Accidental and Unauthorized Activities

Some privacy literature discusses accidental disclosure under the heading of unauthorized disclosure. However, there is a marginal gap between accidental and unauthorized activities. The criteria applied in this paper for distinguishing accidental activities from unauthorized activities are the intention and motive of parties involved. The violation of explicit instructions to follow certain procedures or not to perform certain activities falls into unauthorized activities. In addition to that, performing with the knowledge of the negative consequences that could result from an activity and deliberately neglecting to implement appropriate preventive measures come under the unauthorized category. Accidental activities are mainly due to human errors. Privacy invasive activities carried out with innocent mind and without knowing negative consequences fall into the accidental category. This distinction is important for designing and developing protection measures.

2 ACCIDENTAL ACTIVITIES

Accidental activities take two forms: accidental loss and accidental disclosure of personal information. Section 2.1 and Section 2.2 are dedicated to the accidental loss and the accidental disclosure of personal information respectively.

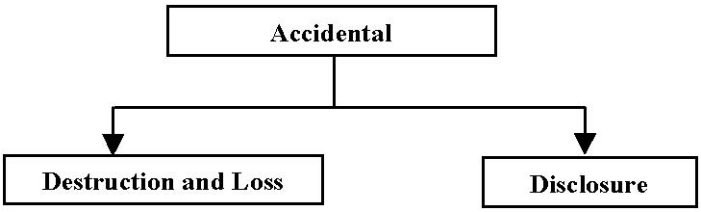

Figure 1: Accidental activities

2.1 Accidental Destruction and Loss

This sub-section discusses the accidental destruction of physical media and the accidental loss of physical media. In the former case, the physical device is with custody but data cannot be recovered. In the second case, the physical media is not in the custody.

It is the duty of data controllers to take appropriate measures to protect physical devices from accidental destruction. This is very important in information privacy since data controllers are required to maintain up-to-date personal information. This position is also stressed in Article 6 of the EU Directive 95/46/EC. The physical storage media range is from papers to cutting edge storage devices. The Australian privacy commissioner stated that the ACT Department of Corrective Services had not taken precautionary measures against deterioration of thermal papers (Privacy Commissioner Tenth Annual Report- Australia, 1998).

There were no cases reported in the studied literature on accidental destruction of technological storage devices. However, all information security standards state the importance of protecting physical storage media from accidents. Common measures are taking backups and storing them in protected places.

According to the OECD privacy guidelines, another cause for losing personal information is the loss of physical devices that contain personal information. The loss of physical devices takes two forms. One is revealing personal information contained in the media and the other one is the mere loss of physical media. Information privacy professionals are keen on the loss of physical media that may reveal personal information. For example, when it is very clear that the motive of a theft is the monitory value of the equipment and not the value of personal information contained therein, there is no information privacy threat. The Australian federal privacy

commissioner took a soft approach (Privacy Commissioner Ninth Annual Report-Australia, 1997) in a case where there was no evidence of accessing sensitive personal information contained in stolen hard drives. On the other hand, if there was a possibility of leaking personal information, the commissioners would have taken it seriously. A Hong Kong bank collected applications for credit cards together with copies of national identity cards on a public holiday. The officer responsible for handing over the collected documents to the bank accidentally left the collected forms and copies of identity cards behind on the bus while taking them home. The applicants complained to the Hong Kong privacy commissioner (HG-ar0304-7, 2004). The commissioner insisted that the bank take proper security safeguards in handling personal information. One of the proposed measures is handing over collected applications to the nearest, safest place.

Media often reports stolen laptops that contain personal information. In a Canadian case, the commissioner suggested some precautionary measures that include implementing proper access control mechanisms and encrypting data (PIPEDA 289,2005). Some other organizational measures are to limit taking laptops containing personal information out of office premises, requiring a prior approval before taking the laptops out of the office, verifying the appropriateness of measures taken before granting approvals, and preventing employees from leaving laptops unattended, specially in vehicles where they can be seen.

2.2 Accidental Disclosure

It can be seen in the following section that causes for accidental disclosure are a lack of knowledge and awareness, human errors, carelessness, and negligence. The Canadian privacy commissioner has stated that it is a duty of data controllers to taka appropriate measures to prevent unauthorized disclosure resulting from employees' mistakes. In taking preventive measures, the controllers have to take into account the sensitivity of personal information and the possibility of disclosure (PIPEDA 180, 2003). In addition to the above-mentioned points, all unexpected situations that lead to the disclosure of personal information are discussed in this sub section.

In many cases, accidental disclosures take place when there is a transmission of personal information. Several cases have been reported on revealing personal information in the conventional postal mail system. This

is due to sending sensitive information in unsealed envelopes (PIPEDA-154, 2001), sending mail to wrong recipients (PIPEDA-28, 2002), printing sensitive information on envelopes, and placing sensitive information in a visible manner through envelope windows (Settled case 9, 2003). The Lithuanian data protection commissioner has insisted on sending public utility service bills in sealed envelopes (WP-29, 2006). To guarantee all mail is properly sealed, the Canadian privacy commissioner suggested checking seals on outgoing message at an outside facility (PIPEDA 197, 2003). Sending an email message is risky since an ordinary email message goes in a clear text format. The Dutch data protection commissioner has advised Dutch libraries to send encrypted email messages to their library members because this communication carries personal information, particularly preferences on library books (WP-29, 2006).

Sending messages to unintended recipient is a serious issue. This is common in the case of facsimile communication. This is largely due to many people sharing a fax machine and not having a cover to conceal the content. In reported case in Hong Kong, a fax copy containing sensitive personal information was sent to a wrong fax number. The sender's sensitive personal information was leaked since the message was collected by an unintended recipient (HG-ar0102-5, 2001). This case highlights the importance of dialling the correct number of the receiving fax machine. A Canadian employee alleged that his employer had intercepted and read a fax receipt. After the inquiry, the privacy commissioner appreciated the guidelines given for fax users on the company's internal web site. It advised fax users to make sure not to leave the document in the sending fax machine and not to send fax messages to unattended fax machines (PIPEDA 251, 2003).

Today, email is the most common means of communication. It is empowered with a number of new features that are not available through conventional communication means. Some features are mail forwarding, replying, and forwarding to multiple recipients. A company sent an email to 618 recipients about a photography contest. Since all mail recipients' addresses were placed in the "to" field, everyone got to know other members in the programme. The company was instructed to create a group email address for all recipients and send mails to that group email address instead of putting all email address in the "to" field (PIPEDA 277,2003). In this case, only the group email address appears. Other possible

vulnerabilities are forwarding to the wrong email addresses, forwarding without deleting sensitive personal information, and placing sensitive personal information in the "subject" field. The latter is especially concerning because the content of the subject field never gets encrypted even in encrypted email messages. Care must be taken in sending electronic documents since it is possible to include personal information in a hidden manner.

There is a possibility of sending an email message to a wrong recipient. It was reported that an email address was assigned to two persons at different times. In this case the parties, who knew the previous email holder, were not informed about the subsequent change. Without knowing the change of holders, an email message containing personal information was sent. This message went to the second owner who was not the intended receiver. Consequently, the sender's personal information was revealed (Computable, 2007). The Italian data protection authority has insisted that police authorities use digital identities of recipients (WP-29, 2006). In addition to that, the double verification system suggested by the Canadian privacy commissioner for the postal mail system (PIPEDA 28, 2002) provides protection from sending email messages to unintended recipients.

Revealing previous users' information is another threat to information privacy. This could happen due to the improper design of data collecting and recording procedures and technological vulnerabilities. One means of collecting users/visitors information is asking them to fill out a row in a registry. In such a data collecting system, there is a possibility of revealing previous users' information. This issue is highlighted in a Canadian case (PIPEDA 304, 2005). In this case, visitors were asked to write their names at the entrance to a movie theatre. The Canadian privacy commissioner ruled out this procedure since it led visitors to notice the previous users' information and asked the movie theatre to give each visitor a form to write down particulars. It seems this problem was solved in the electronic data collecting system. However, there are some reported cases where this problem occurred in a different manner due to the lack of awareness, poor designing of information systems, and negligence. For example, it can be seen that many users leave their computers, web browsers, and sensitive accounts such as email accounts, bank accounts open without properly logging off. Some users are not aware of threats and others simply ignore this for convenience. Leaving without proper logging off is a problem in

publicly accessible computers, particularly machines in cyber cafes. Possible means of overcoming this problem is proper awareness campaigns and trainings on possible threats and protection measures. Proper design of technological solutions could solve these kinds of vulnerabilities to a great extent.

Even though there are decisions that state it is not necessary to send registered mail (PIPEDA 43, 2002), the Australian privacy commissioner insisted on getting signatures on a delivery receipt (J v Superannuation Provider, 2006). Therefore, it can be expected that getting an email delivery report would give a kind of guarantee that the message was been delivered to the intended recipient. However, there is a possibility of sending an acknowledgement by a third party.

Another identified information privacy threat is using collected personal information for training, educational, and promotional campaigns. Unless the collected personal information is carefully scrutinized and de-identified, it poses threats to data subjects. A company developed a case study based on the facts collected from a couple for marketing purposes. In the process of building the marking plan, some identifiable information was not taken off. Subsequently, the couple realized their personal information was contained in the marketing plan. They then complained to the privacy commissioner. In the inquiry, the company admitted its mistakes and promised to take precautionary measures. One of those measures is not to build further marketing plans based on particulars of customers (NZPrivCmr2-26280, 2002). A possible threat in the digital world is using databases containing personal information for educational, training, and testing purposes.

Another important area is providing access to data repositories that contain personal information to IT service agencies. It is the responsibility of the principle, not the agency, to protect personal information (PrivCmrNZ6-2663, 1994). Outsourcing business processes that contain personal information is a serious threat. It is suggested to have strict contractual terms with data processors. According to Article 16 and 25 of EU Directive 95/46/EC, sending personal information without having a proper contractual term with data processors is prohibited.

Some reported cases highlight the limitation of technological systems. An erroneous match took place since a mother and her son have the same initials in addition to surname and address. This erroneous matching

disclosed the son's personal information. Thereafter, the company decided to put the son's name to a manual monitor list where an employee checked the entries manually each month (PIPEDA 150, 2003).

Taking proper administrative measures is essential for protecting personal information from accidental disclosures. Some recommended measures are having a close place to deal with customers (PIPEDA 237,2003), having working desks with raised barriers at chest level to prevents seeing personal information and instructing employees not to speak loudly (PIPEDA 245, 2003). It is also essential to follow proper security procedures when discarding personal information. In one case, personal information of a worker was revealed because the organization had failed to follow proper procedures in discarding binders. The investigation showed the limitations of security procedures (PIPEDA 228, 2003).

Not only organizations but also data subjects have a duty to help keep data subjects' personal information secure. Some times, data subjects put their personal information at risk by failing to follow given security procedures. In a Canadian case, a worker accompanied her co-worker to a clinic's reception area and later alleged that the receptionist disclosed her personal information to the accompanied co-worker. The commissioner turned down the complaint since the clinic had followed proper security procedures (PIPEDA 237, 2003). Another case was turned down since a user had chosen her mother's maiden name for her password despite the instruction given to her not to choose an easy-to-guess password (PIPEDA 315, 2003).

3 DISCUSSION

This study presented an analysis of decisions given on the principle of security safeguards, particularly accidental incidents by data protection and privacy commissioners. It covered the Ninth Annual Report of the Article 29 Working Party on Data Protection and decisions published online by the Canadian, Hong Kong, New Zealand, and Australian privacy commissioners. This study shed light on how to understand the legal privacy obligations of data controllers in case of accidental incidents. Furthermore, it presented some implementation details of technological measures and appropriate organizational measures for managing technological measures.

Unlike existing privacy frameworks, best practices, and guidelines, the recommendations presented in this paper are meant to have legally binding

effects. This is because these guidelines were derived from verdicts given by data protection and privacy commissioners along with other legally competent tribunals. Therefore, it can reasonably be said these guidelines are mandatory legal privacy requirements. However it should not be expected that these guidelines have the same level of legally binding effects in all jurisdictions as there is no universal harmonized data protection regime. Because all of the studied verdicts were geared toward protecting personal information, it can reasonably be claimed that adhering to measures presented in this paper will contribute to the enhancement of information privacy.

4 REFERENCES

1 [AICPA/CICA] Assurance Services Executive Committee of the AICPA and the Assurance Services Development Board of the CICA. (2004). AICPA/CICA Privacy Framework. New York: Author.

2 APEC. (2005). APEC Privacy Framework -APEC Secretariat-. Retrieved November 30, 2007, from www.apec.org.

3 Computable. (2007). Online identiteit gestolen- 19th of October- Computable. Retrieved November 30, 2007, from www.computable.nl/nieuws.

4 Dempsey, J. X., & Rubinstein, I. (2006). Guest Editors' Introduction: Lawyers and Technologists-Joined at the Hip? IEEE Security and Privacy, 4(3), 15-19.

5 GH-2004005. (2004). Senders of information through fax: must ensure no unauthorized or accidental access to the information by unrelated parties. Retrieved November 30, 2007, from http://www.pcpd.org.hk/english/casenotes/

6 Greenleaf, G., & Waters, N. (2003). The Asia-Pacific Privacy Charter Retrieved November 30, 2007, from http://www.worldlii.org/int/other/PrivLRes/2003/1.html#Heading1

7 HG-Annual Report. (2006). Personal DataAnnual Report 2004-05 Retrieved November 30, 2007, from http://www.pcpd.org.hk/english/publications/annualreport2005_4.html

8 HG-ar0102-5. (2001). Wrongful transmission of subscribers' personal data by fax. Retrieved November 30, 2007, from www1.pco.org.hk/textonly/english/casenotes/case_complaint2.php?id=156

9 HG-ar0304-7. (2004). Retrieved November 30, 2007, from

www1.pco.org.hk/textonly/english/casenotes/case_complaint2.php?id=202
10 Iachello, G. (2003). Protecting Personal Data: Can IT Security Management Standards Help? In Proceedings of the 19th Annual Computer Security Applications Conference (Vol. 8, pp. 266 - 275). Washington, DC: IEEE Computer Society.
11 J v Superannuation Provider. (2006). Improper disclosure of personal information and failure to take reasonable steps to protect, and correct personal information. Retrieved November 17, 2007, from www.privacy.gov.au/act/casenotes/2005.html
12 Muelle, G., & Rannenberg, K. (1999). IT Security and Multilateral Security In K. Rannenberg,
A. Pfitzmann & G. Müller(Eds.) Multilateral Security in Communications. Boston, MA: Addison¬Wesley-Longman.
13 NZPrivCmr2-26280. (2002). Clients object to their financial report being used for marketing purposes by life assurance company. Retrieved November 30, 2007, from
http://www.privacy.org.nz/library/
14 OECD. (1980). OECD Guidlines on the protection of Privacy and Transborder Flows of Personal Data. from http://www.oecd.org/document /20/0,2340,en_2649_201185_15589524_1_1_1_1,00.html
15 Opinion 1/98. (1998). Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS). Retrieved September 04, 2007, from
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en .htm
16 PIPEDA-154 (2001). Couple dismayed at receiving unsealed envelope from bank. Retrieved November 30, 2007, from http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030415_1_e.asp
17 PIPEDA 43 (2002). Credit card fraud victim questions bank's use of first-class mail as privacy safeguard. Retrieved November 30, 2007, from http://www.privcom.gc.ca/
18 PIPEDA 150 (2003). Credit agency accused of improper disclosure of personal information. Retrieved November 30, 2007, from http://www.privcom.gc.ca/cf-dc/2003/ cf-dc_030411_2_e.asp
19 PIPEDA 180 (2003). Bank uses tape-recording of customer's call for unidentified training purpose; connects another customer to the recording. Retrieved November 30, 2007, from http://www.privcom.gc.ca/cf-dc/2003/ cf-dc_030710_02_e.asp

20 PIPEDA 197 (2003). Individual alleged bank sent personal information in unsealed envelopes. Retrieved November 30, 2007, from http://www.privcom.gc.ca/cf-dc/2003/ cf-dc_030801_02_e.asp
21 PIPEDA 227 (2003). Mass mailout results in disclosure of contest entrants e-mail addresses. Retrieved November 30, 2007, from http://www.privcom.gc.ca/cf-dc/2003/ cf-dc_040902_02_e.asp
22 PIPEDA 228 (2003). A transportation company disclosed an employee's personal information without consent. Retrieved November 30, 2007, from http://www.privcom.gc.ca/cf-dc/2003/ cf¬dc_031104_03_e.asp
23 PIPEDA 237 (2003). Individual accuses employer of disclosing personal information to co¬workers. Retrieved November 30, 2007, from http://www.privcom.gc.ca/cf-dc/2003/cf¬dc_031120_02_e.asp
24 PIPEDA 245 (2003). Bank alleged to have unnecessarily collected and improperly disclosed personal information. Retrieved November 30, 2007, from http://www.privcom.gc.ca/cf-dc/2003/ cf-dc_031203_e.asp
25 PIPEDA 251 (2003). A question of responsibility. Retrieved November 30,2007,from http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031212_04_e.asp
26 PIPEDA 254 (2003). Daughter racks up long-distance charges; mom blames phone company. Retrieved November 30, 2007, from http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031223_e.asp
26 PIPEDA 289 (2005). Stolen laptop engages bank's responsibility. Retrieved November 30, 2007, from http://www.privcom.gc.ca/cf-dc/2005/289_050203_e.asp
27 PIPEDA 304 (2005). Movie theatre chain strengthens personal information handling practices. Retrieved November 30, 2007, from http://www.privcom.gc.ca/cf-dc/2005/304_20050607_e.asp
28 PIPEDA 315 (2005). Web-centred company's safeguards and handling of access request and privacy complaint questioned. Retrieved November 30, 2007, from http://www.privcom.gc.ca/cf¬dc/2005/index2-5_e.asp
29 PIPEDA_28 (2002). Bank sends customers' pay stubs to wrong party. Retrieved November 30, 2007, from http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020104_e.asp
30 Privacy Commissioner Ninth Annual Report- Australia. (1997). Retrieved November 30, 2007, from http://www.privacy.gov.au/publications/97annrep.pdf

31 Privacy Commissioner Tenth Annual Report- Australia. (1998). Retrieved November 30, 2007, from http://www.privacy.gov.au/publications/98annrep.pdf
32 PrivCmrNZ6-2663. (1994). Woman complains process server revealed debt details at old address Retrieved November 30, 2007, from http://www.privacy.org.nz/library/
33 Settled case 9. (2003). Windows reveal too much information. Retrieved November 30, 2007, from http://www.privcom.gc.ca/ser/2004/s_040706_e.asp
34 Waters, N., & Greenleaf, G. (2001). Privacy Law and Policy Reporter. Retrieved November 30, 2007, from http://www.austlii.org/au/journals/PLPR/2004/36.html
35 WP-29. (2006). Ninth Annual Report of the Article 29 Working Party on Data Protection. Retrieved November 4, 2007, from http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm