APEC PRIVACY FRAMEWORK SEMINAR

Panel III—Giving Effect to the APEC Privacy Framework (Breakout Sessions)

Hong Kong SAR
Wednesday, June 1, 2005
1400-1530

Case Study 1

Customer opts-out of receiving promotional material but bank continues to send it

Facts of the Case

A customer complained that his bank was not allowing him to withdraw his consent to receive unsolicited advertising materials. The customer alleged that he had opted-out of receiving this material from the bank's businesses, affiliates and subsidiaries on a number of occasions but still was receiving it.

In August 2001, the complainant, a long-time customer of the bank, had received a notice from the bank that included instructions on how to opt-out of receiving unsolicited advertising. The complainant followed those instructions but continued to receive advertising. Some months later, he contacted the bank again. He was told that a "do not solicit" tag was placed on his file. A couple of months later, he received solicitation from one of the bank's affiliates. When he contacted the bank, he was told that, although his file did contain a "do not solicit" tag, he would have to send a letter directly to the affiliate, withdrawing his consent. The complainant refused to do so. Based on the wording in the notice he received and on the bank's opt-out policy contained on its web site, he understood that when he withdrew consent, his withdrawal applied to all of the bank's businesses, affiliates and subsidiaries. He was again assured that his file would be marked "do not solicit" and that the affiliate would also make such a notation on its file. However, in spite of this, the complainant continued to receive advertising materials.

The bank's privacy policy states that the policy applies to the bank, its businesses, affiliates and subsidiaries. The policy states that, if a customer does not wish to receive advertising, he or she can opt-out by contacting his or her nearest branch or by telephoning a toll-free number.

Issue for Discussion

Should the opt-out apply to the original bank, its businesses, affiliates and subsidiaries or only to the original bank?

APEC PRIVACY FRAMEWORK SEMINAR

Panel III—Giving Effect to the APEC Privacy Framework (Breakout Sessions)

Hong Kong SAR
Wednesday, June 1, 2005
1400-1530

Case Study 2

Collection of credit card copies by an airline company from customers

Facts of the Case

An airline company required customers who purchased air tickets by fax / email to provide their credit card information for confirming the transaction. The airline collected the name of credit card holder, the card number, the card expiry date and a photocopy of the credit card. The airline company said that a photocopy of the credit card was required for the purpose of verifying the credit card information filled in by the customer and for preventing any unlawful or seriously improper conduct.

Issues for Discussion

(a) What is the purpose of use of the personal information collected by the airline company?

(b) Is the collection of the credit card photocopy relevant for the purpose of collection?

(c) Is collection of the credit card photocopy proportional to the fulfilment of the collection purpose?

APEC PRIVACY FRAMEWORK SEMINAR

Panel III—Giving Effect to the APEC Privacy Framework (Breakout Sessions)

Hong Kong SAR
Wednesday, June 1, 2005
1400-1530

Case Study 3

Disclosure of customers' information by banks to the police

Facts of the Case

The devastating tsunami that struck the South Asian region in December 2004 resulted in massive loss of life, property and livelihood. Many tourists who had been vacationing in the region were reported missing. Anxious families of the tourists sought help from their domestic governments to find their missing family members. To try to find whether the missing persons had been in the affected areas at the time of the tsunami, police asked banks to provide credit cardholders' information. They asked the banks for information about cardholders whose credit cards had been used in affected areas shortly before the tsunami. The police said they would use that information to verify whether missing persons were in the affected areas to assist with rescue operations.

Issues for Discussion

(a) What is the original collection purpose of credit card holders' information by the banks?

(b) What is the subsequent purpose of use of the information by the police?

(c) Should the banks provide the information to the police? If not, should there be an exemption applicable in the circumstances of the case?

APEC PRIVACY FRAMEWORK SEMINAR

Panel III—Giving Effect to the APEC Privacy Framework (Breakout Sessions)

Hong Kong SAR
Wednesday, June 1, 2005
1400-1530

Case Study 4

Bank customer barred from using e-banking facilities after he rejected cookies

Facts of the Case

A bank customer tried to transfer money from his account online using the e-banking services of his bank. When he logged into the e-banking website, a notice appeared on his computer screen. It told him that cookies would be used to collect certain information of the user, including the websites the user had visited immediately before and after using the e-banking website. The notice stated that the information collected would be used to create personal profiles of customers. The customer decided to reject the cookies and was then immediately barred from using the e-banking service further.

Issues for Discussion

(a) Was the customer given a choice in relation to the collection of his personal information?

(b) If not, was this acceptable? If not, what should the bank do?

APEC PRIVACY FRAMEWORK SEMINAR

Panel III—Giving Effect to the APEC Privacy Framework (Breakout Sessions)

Hong Kong SAR
Wednesday, June 1, 2005
1400-1530

Case Study 5

Incorrect entry of email address resulting in disclosure of personal information

Facts of the Case

A customer of a telephone company called the company to register his email address so he could receive electronic bills. The company's employee incorrectly typed the email address into the company's computer system. This caused the customer's bills to be sent to the wrong person, thereby disclosing information of the customer (such as his calling records). The provider did not have any policy or procedure to double check the data inputted.

Issues for Discussion

(a) Do the APEC Privacy Principles contain anything about this kind of case? Is a simple data entry mistake a breach of the APEC Privacy Principles?

(b) What could the telephone company do in future to ensure accuracy of data entry?