***PIPEDA* Case Summary #319**

ISP's anti-spam measures questioned

(Section 2; Principle 4.3)

Complaint

The complainant alleged that his internet service provider (ISP) was reading his outgoing e-mail messages and, as a result, was declining to route them if they were not destined to travel through the ISP's mail servers.

Summary of Investigation

The complainant subscribed to the ISP's high-speed internet service. He also subscribed to a web-centred company's third-party e-mail service, which allows individuals to send and receive e-mail messages from external mail accounts. The complainant was upset because he could not send e-mail without going through his ISP's mail servers.

The complainant contacted his ISP about this matter. The ISP stated that it was making its customers use its outgoing mail server because it has anti-spam measures in place. It maintained that as a responsible network administrator it had to implement network security measures to protect its network and its users.

The complainant was concerned that in order to route outgoing mail through its mail servers, the ISP was inspecting and screening his outgoing e-mails without his consent. He stated that his ISP's technical support staff told him that it was "snooping" into the user portion (TCP portion) of a packet and when the specific field for the TCP Port was set to 25, the ISP was blocking access to outside e-mail servers. He believed that the port information is indivisible from the rest of the packet; therefore, by reading the port address, the ISP was reading the entire e-mail.

The ISP stated that its automated systems must identify elements of a packet (i.e. the address and port information) in order to correctly route the message and provide basic e-mail service. It added, however, that there is no inspection of the content of the packet stream at all, aside from the standard inspection of the source and destination IP address in order to make a routing decision, and the inspection of the source and destination TCP port addresses.

If the port address is 25, the ISP will identify the destination IP address to make sure that the e-mail is being routed through its mail server. The complainant was trying to route his e-mails through the outside mail server, and he believed that his ISP did not have the right to know that he was using the other web-centred company as a third-party mail provider.

The ISP stated that it blocks e-mail messages that are not bound for its mail servers. If e-mail traffic does not go through its mail servers, then it also bypasses the spam filtering mechanisms that would combat spam. Blocking e-mail from port 25 is in keeping with Industry Canada's Spam Task Force's Recommended Best Practices for Canadian ISPs and Other Network Operators. The complainant indicated that he believes he has the right to send spam as there is no law against it, only the aforementioned best practices.

The ISP stated that it is looking for TCP 25 in a packet header's destination port field. If the packet is marked with a destination port of TCP 25 and has a destination IP address of any network other than the ISP's mail servers, the packet is deleted. In other words, the message is not routed. Under the terms of service that the complainant agreed to as a residential high-speed customer, all e-mail must be routed through the ISP's mail servers.

The company's acceptable use policy for internet access services prohibits the customer from engaging in or assisting others to engage in any activity that violates applicable policies, rules or guidelines of the ISP or of other on-line service providers, including the posting, uploading, reproducing, distributing, otherwise transmitting, or collecting of spam. The customer is also prohibited from engaging in any conduct that directly or indirectly encourages, facilitates, promotes, relies upon or permits such prohibited activities including failing to implement reasonable technical or administrative measures to prevent spam.

The ISP's internet services account agreement states that the user acknowledges having read the ISP's privacy commitment, and that the user consents to the collection, use and disclosure by the ISP of personal information collected in connection with the provision or use of the ISP's internet services, solely for the purposes identified in the privacy commitment. According to the ISP's privacy commitment, it collects personal information for the purpose of providing service.

The agreement also states that the user agrees that the ISP has the right to, without notice, monitor use of the ISP's internet services and monitor, review and retain such content, material or information if ISP believes in good faith that such activity is reasonably necessary to provide the ISP's internet services to customers.

Although at first the complainant denied ever accepting the terms of service, the ISP provided the Office with evidence to the contrary, in the form of a printout from its billing system that shows the complainant accepted the terms on three separate occasions, the first being when he originally signed up for high-speed service in December 2002. He also received a welcome e-mail that references the terms. He nevertheless contended that, although he accepted the terms of service agreement, he was not aware of the terms.

Findings

Issued November 8, 2005

Application: Section 2 states that personal information is "…information about an identifiable individual…." Principle 4.3 stipulates that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

In making her determinations, the Assistant Privacy Commissioner deliberated as follows:

- The first issue the Assistant Commissioner considered was whether any of the information under discussion in this complaint could be considered "personal information" as defined in section 2.
- In her view, an IP address can be considered personal information if it can be associated with an identifiable individual.
- In the complainant's case, he is assigned a dynamic IP address, which means that it changes each time he logs on. This IP address was associated with the particular computer he was using.
- The ISP does not identify the user before he or she is allowed to send e-mail, but ensures that the user is directly connected to the ISP network and is therefore a customer of the ISP.
- For the purposes of this complaint, which involved the sending of e-mail by the complainant, the Assistant Commissioner accepted that the originating IP address identified the complainant and was therefore his personal information, as per section 2.
- The ISP needs to know the destination IP address in order to deliver the message that is being sent. A port address, however, is not personal information as it is not linked to an identifiable individual.
- The complainant accepted the terms of the service agreement, which specify that the ISP collects and uses personal information for the purpose of providing service. By virtue of sending e-mail, the complainant also consented to the ISP reading the IP addresses to route the mail.
- She therefore did not find the ISP in contravention of Principle 4.3 when it reads the originating IP address.
- As for the allegation that the ISP reads the contents of the entire e-mail packet without the complainant's consent, the Assistant Commissioner determined that there was no evidence to suggest that this was the case.
- The ISP denied that it reads anything apart from the IP and port addresses (the latter is not personal information). When the port information on the address is read, it is read by the ISP's mail servers, electronically. No person actually reads the e-mail in this process.
- The process of reading and routing e-mail address information does not require the servers to access or read the user portion of the e-mail. The software program is set to access a predetermined portion of the address, and therefore this is the only portion of the address that is read.
- The Assistant Commissioner therefore found that the ISP did not contravene Principle 4.3.

She therefore concluded that the complaints were not well-founded.