Security firm and police criticised for street CCTV

Report by Eugene Oscapella

ON TWO THORNY SURVEILLANCE ISSUES, George Radwanski, Canada's Federal Privacy Commissioner has taken a stance that may resonate in other jurisdictions facing similar issues.

The Commissioner has concluded that a company's video surveillance of a public place violated fair information practices – specifically, the principle prohibiting collection of personal data without the consent of the individual. He also sharply criticised similar surveillance by Canada's national police force, the RCMP.

As a marketing demonstration, a security company in Canada's Northwest Territories had mounted four video cameras on the roof of its office building. The cameras pointed at a main intersection of the capital city of Yellowknife. For several days, company staff monitored live feed from the street 24-hours a day. On several occasions, staff noted incidents and reported them to police.

By the company's own admission, this surveillance activity was a marketing demonstration intended to generate business. As a result of the negative publicity, the company removed the cameras less than a week after they had been installed.

In his most recent annual report to Parliament, the Privacy Commissioner concluded that: "There may be instances where it is appropriate for public places to be monitored for public safety reasons. But this must be limited to instances where there is a demonstrable need. It must be done only by lawful public authorities and it must be done only in ways that incorporate all privacy safeguards set out by law. There is no place in our society for unauthorised surveillance of public places by private sector organisations for commercial reasons."

The fact that the video feed was live and not taped was irrelevant, since Canada's recently enacted Personal Information Protection and Electronic Documents Act does not restrict personal information to recorded information. The Commissioner was satisfied that the company had collected personal information without consent.

The Commissioner also investigated the use of video surveillance cameras by the RCMP in one small British Columbia community. The RCMP was continuously monitoring and recording everyone on a public street. He found this to be in clear contravention of the Privacy Act, which covers personal information held by the Government of Canada. The RCMP is still continuing 24-hour surveillance, only now without continuous recording.

The Commissioner concluded that eliminating the recording process technically complied with the Privacy Act, which defines personal information as information about an identifiable individual that is "recorded in any form".

Nonetheless, he called this sort of video surveillance of public places "an extremely serious violation of privacy rights even in the absence of recording. It is the very presence of video cameras, whether they are recording at any moment or not, that creates the privacy-destroying sense of being observed."

Further information: Privacy Commissioner of Canada, Annual Report to Parliament, 2000-2001: www.privcom.gc.ca/information/ar/02_04_09_e.asp

Security fixes for Windows XP and AOL

The *Washington Post* reported on January 4th that the FBI was satisfied that a software "patch" offered by the Microsoft Corporation was sufficient to fix a major security weakness discovered in the Windows XP operating system. The newspaper reported that the vulnerability – "a kind of open door to the Internet" – would allow a hacker to seize control of a computer when it connected online, enabling the intruder to steal information or launch a virus attack on other computers.

Microsoft posted a patch that corrects the problem on its website the day the problem was reported, but the FBI urged computer users to take the extra precaution of disabling the Windows XP feature that created the vulnerability. The FBI has since reversed its position, saying that it was satisfied with the patch.

On January 2nd, the online news service Wirednews reported a statement by AOL that it had closed a security hole in its Instant Messenger (AIM) application. This fault could have given hackers access to, and control over, Windows PCs running the latest version of AIM.

For further information: www.washingtonpost.com/wp-dyn/articles/A59101-2002Jan3.html and www.wired.com/news/technology/0,1282,49442,00.html